Course Outline

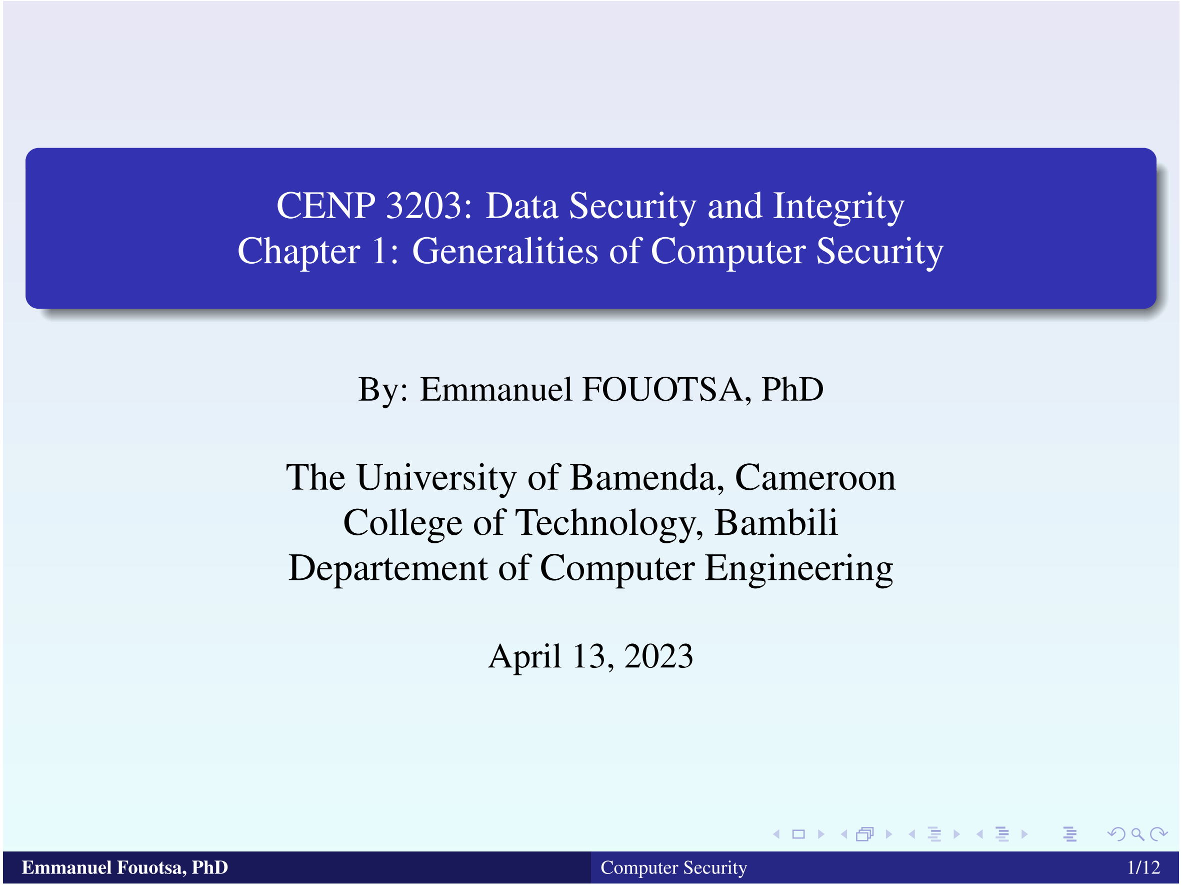
School : College of Technology **Department** : Computer Science Engineering
Course Title: Data Security and Integrity **Course Code: CENP 3203**
Semester: 4 Day: **Time: Credit 3 (30-15-00)**
Instructor: Dr. Emmanuel Fouotsa, Lecturer **Office/ Hours:**
Lecturer's Web page: www.emmanuelfouotsa-prmais.org E-mail : emmanuelfouotsa@yahoo.fr,

Course Description and Content: This course provides students with a background, foundation, and insight into the subject of Computer Security at a graduate level. It covers Basic principles about security models Security for operating system , Information security, Data Security , System security, Introduction to encryption, Security services, Confidentiality, Authentication, Integrity, Access Control , Threats and risks such as for example, - Viruses, troyans, worms, Web security, Database security, Network security, IDS systems, Security evaluation.
Course Objectives and outcomes: After completing this course a student should be able to:
1- on the basis of a company's policy write security policy with considerations to confidentiality, integrity and availability that describes directives and documents and define for user and using computer systems.
2- Identify, describe and analyse threat and risks for different systems
3- have basic knowledge about security mechanisms and security services, encryption techniques, IDS and firewalls, network security
4- be familiar with the malicious of different types programs and countermeasures

Bibliography:

1- **National Institute of Standards and technology: An introduction to computer security: The NIST Handbook, 1995**
2- **Joseph Pierprzyk, Thomas Hardjono, Jennfer Sebeony: Fundamentals of computer security, Springer 2003**

Week	Slot		TOPICS	ACTIVITY		
	Day	Time		L	T	P
1			Part 1: Basics in computer security Terminology (Computer security, threats, attacks..)	3	0	
2			The security attacks	3	0	
3			Security services/requirements and security mechanisms/strategies	3	0	
4			Part 2: Principle of Computer Security User authentication (Principle, Password, token, biometric based authentication)	3	2	
5			Access control	3	2	
6			Malicious Software (Viruses, worms, Trojans, zombie, spam, phishing,……	3	0	
7			Intrusion detection/prevention and firewalls	4	3	
8			Denial of service attacks (Principles, examples defences)	3	1	
9			Introduction to cryptographic algorithms to ensure security(Encryption technics,...)	3	1	
10			Presentation of exposés and projects on : OS security/Software security, Database security, cloud security	0	4	
11			Presentation of exposés on Internet security protocols, wireless networks security, Network security.	0	2	
12			Final remarks and preparation to the final year exam	2	0	

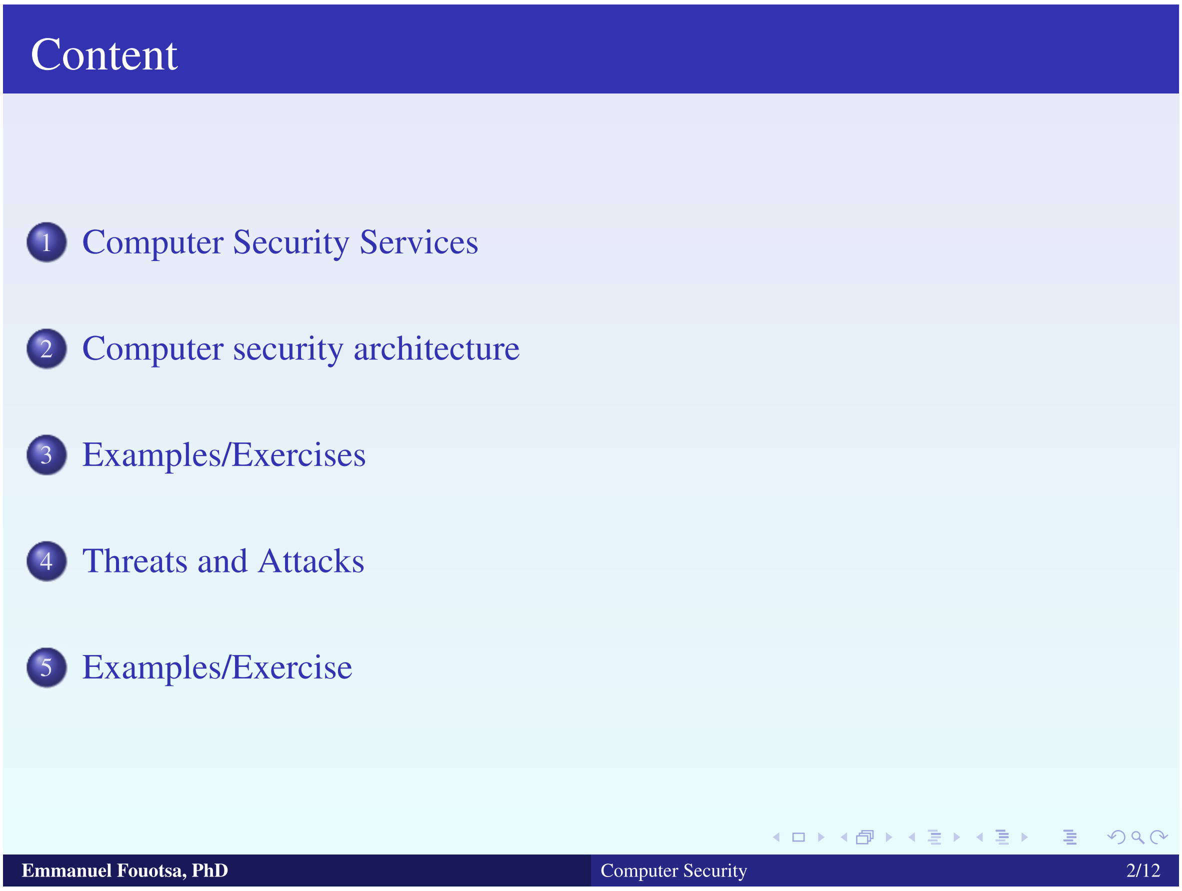


CENP 3203: Data Security and Integrity
Chapter 1: Generalities of Computer Security

By: Emmanuel FOUOTSA, PhD

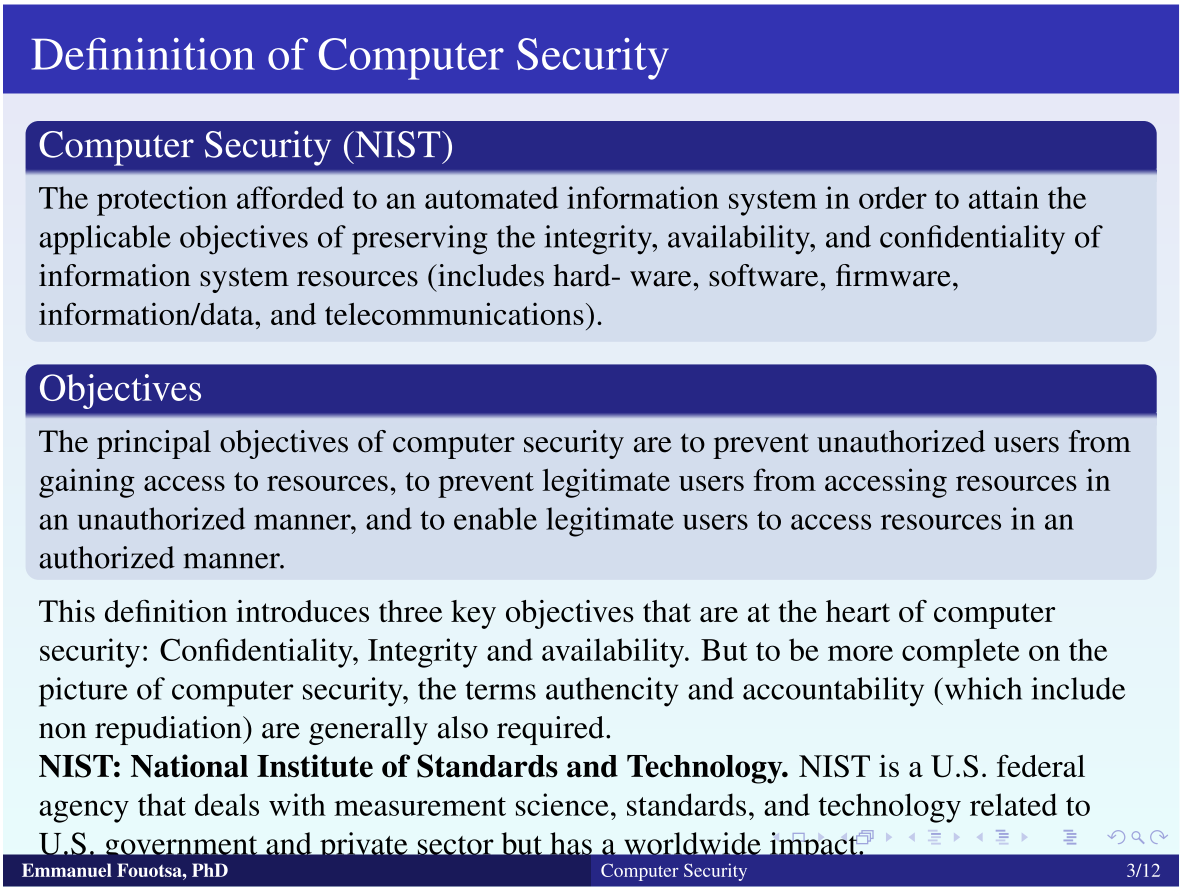
The University of Bamenda, Cameroon
College of Technology, Bambili
Departement of Computer Engineering

April 13, 2023



Content

1. Computer Security Services
2. Computer security architecture
3. Examples/Exercises
4. Threats and Attacks
5. Examples/Exercise



Defininition of Computer Security

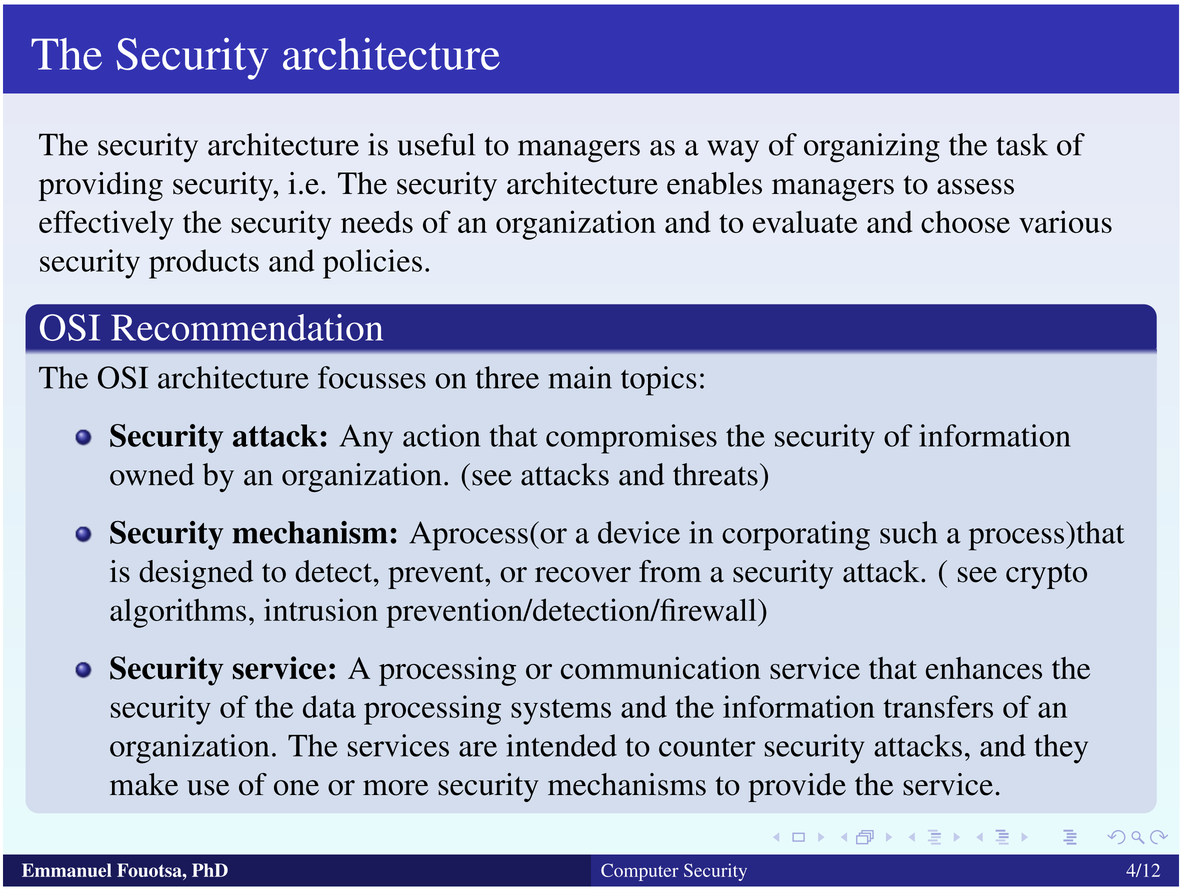
Computer Security (NIST)

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hard- ware, software, firmware, information/data, and telecommunications).

Objectives

The principal objectives of computer security are to prevent unauthorized users from gaining access to resources, to prevent legitimate users from accessing resources in an unauthorized manner, and to enable legitimate users to access resources in an authorized manner.

This definition introduces three key objectives that are at the heart of computer security: Confidentiality, Integrity and availability. But to be more complete on the picture of computer security, the terms authencity and accountability (which include non repudiation) are generally also required.
NIST: National Institute of Standards and Technology. NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government and private sector but has a worldwide impact.



The Security architecture

The security architecture is useful to managers as a way of organizing the task of providing security, i.e. The security architecture enables managers to assess effectively the security needs of an organization and to evaluate and choose various security products and policies.

OSI Recommendation

The OSI architecture focusses on three main topics:

- **Security attack:** Any action that compromises the security of information owned by an organization. (see attacks and threats)
- **Security mechanism:** Aprocess(or a device in corporating such a process)that is designed to detect, prevent, or recover from a security attack. (see crypto algorithms, intrusion prevention/detection/firewall)
- **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

What is OSI

OSI

OSI: The International Organization for Standardization is a world- wide federation of national standards bodies. ISO is a nongovernmental or- ganization that promotes the development of standardization and related activities with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scien- tific, technological, and economic activity. ISO's work results in international agreements that are published as International Standards.

Security Services

- **Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity:** Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
- **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Security Services: Cont.

- **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or messageoriginator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Because truly secure systems are not yet an achiev- able goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

Examples/Exercise

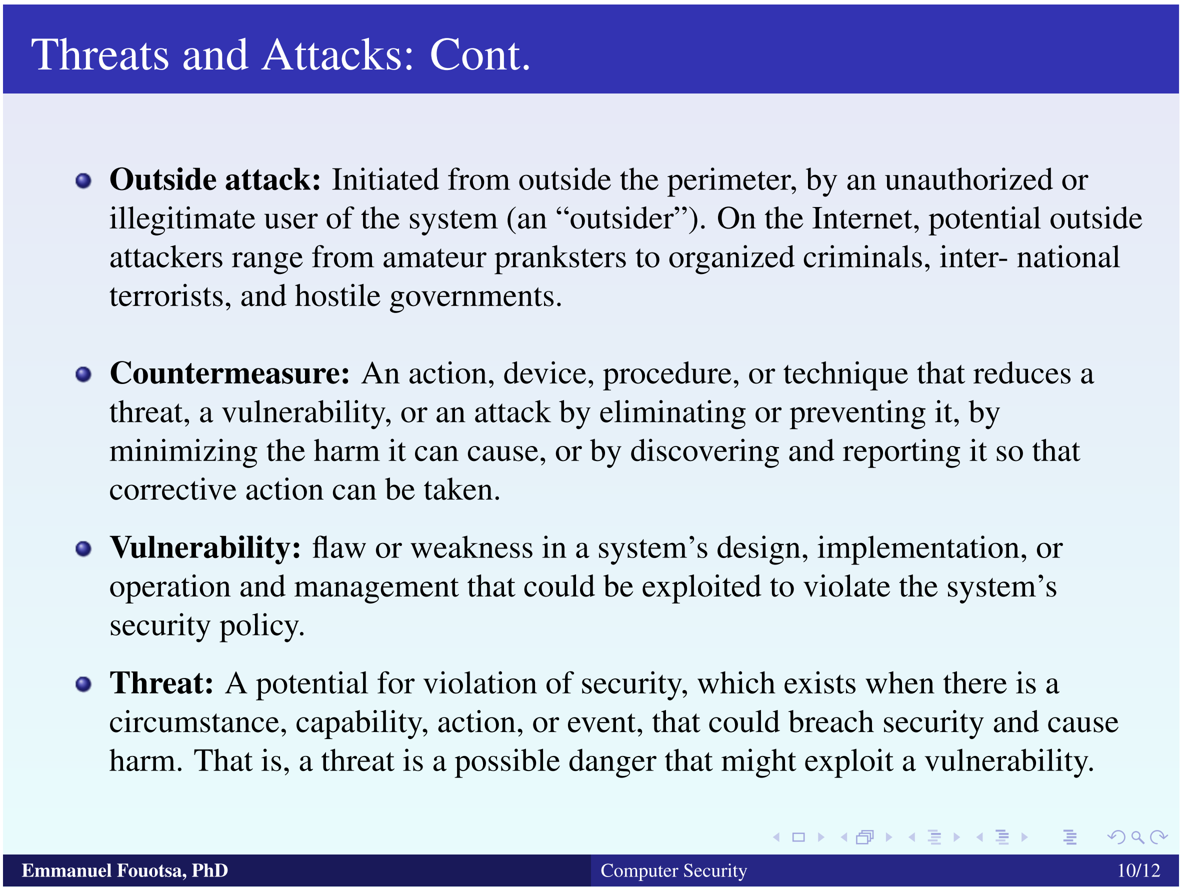
For each of the following fields list some examples of applications that illustrate the requirements just enumerated

- Health services
- Army
- University
- Telecommunication
- Administration
- Banking

Threats and Attacks

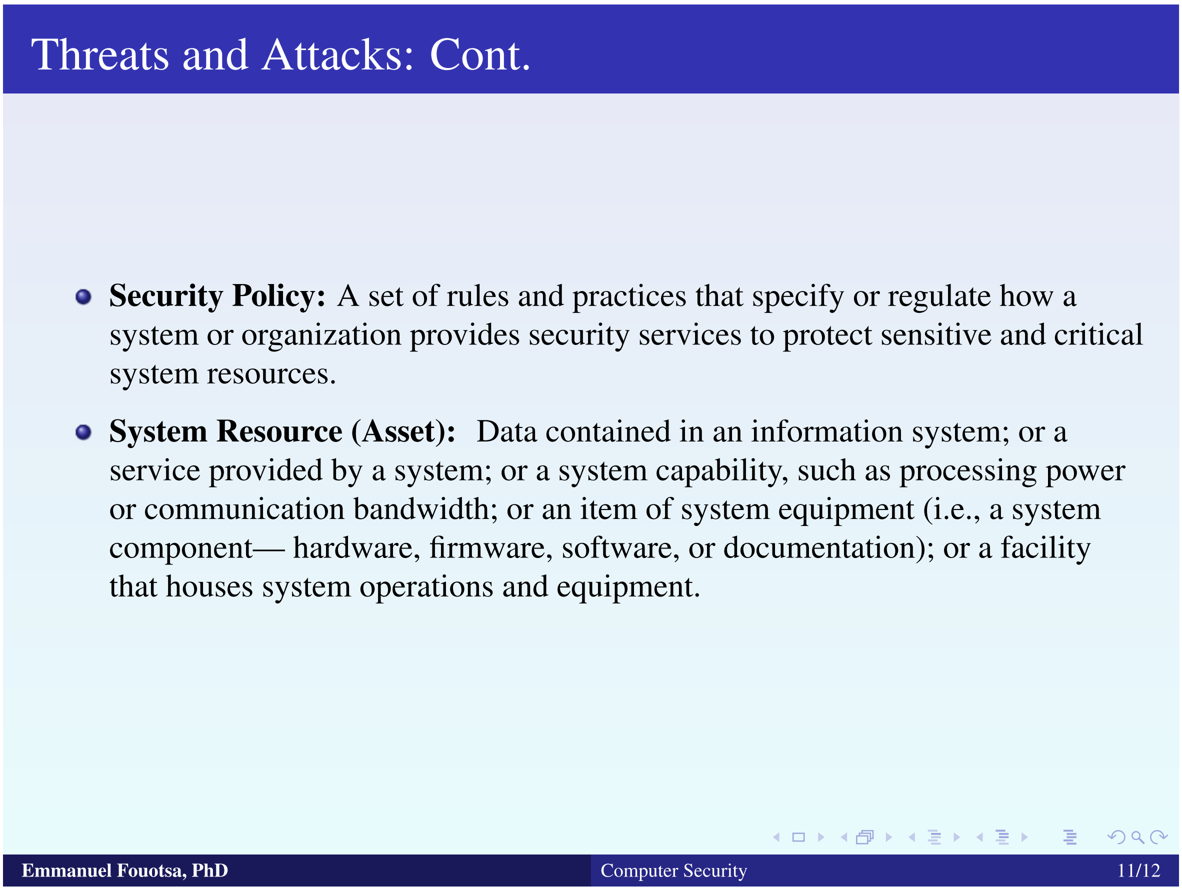
In this section we introduce some terminology related to computer security. These definitions are from the **Internet Security Glossary**.

- **Data:** Any object that can be processed or executed by a computer
- **Adversary or threat agent:**An entity that attacks, or is a threat to, a system. It is the agent carrying out an attack
- **Attack:** An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system. We distinguish two type of attacks or types of attacks based on their origin:
    - **Passive attack:** An attempt to learn or make use of information from the sys- tem that does not affect system resources.
    - **Active attack:**An attempt to alter system resources or affect their operation.
    - **Inside attack:** Initiated by an entity inside the security perimeter (an “insider”). The insider is authorized to access system resources but uses them in a way not approved by those who granted the authorization



Threats and Attacks: Cont.

- **Outside attack:** Initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an “outsider”). On the Internet, potential outside attackers range from amateur pranksters to organized criminals, inter- national terrorists, and hostile governments.
- **Countermeasure:** An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.
- **Vulnerability:** flaw or weakness in a system’s design, implementation, or operation and management that could be exploited to violate the system’s security policy.
- **Threat:** A potential for violation of security, which exists when there is a circumstance, capability, action, or event, that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

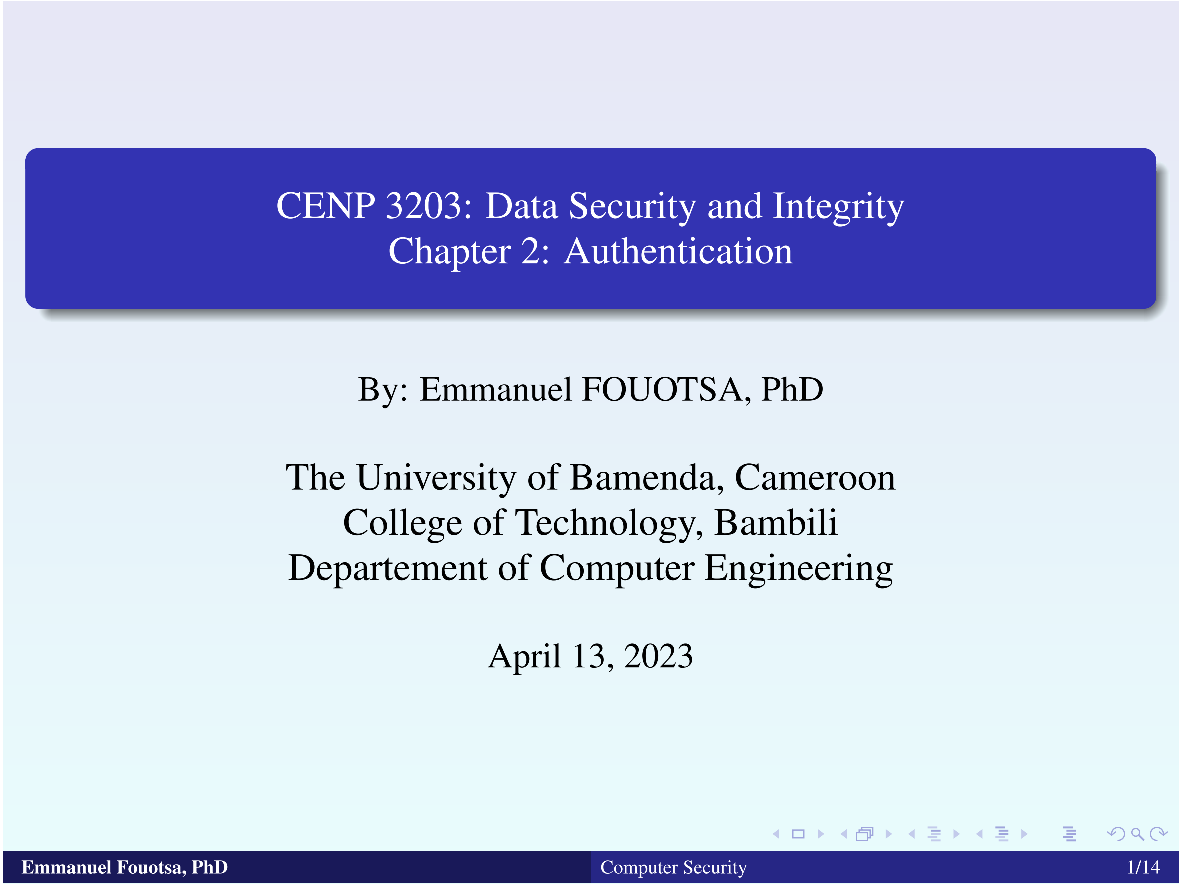


Threats and Attacks: Cont.

- **Security Policy:** A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.
- **System Resource (Asset):** Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component— hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

Examples/Exercise

For each of the computer and network assets: *Hardware*, *Software*, *Data*, *Communication lines and Networs*, describe threats to the following security requirements: Availability, confidentiality, integrity.

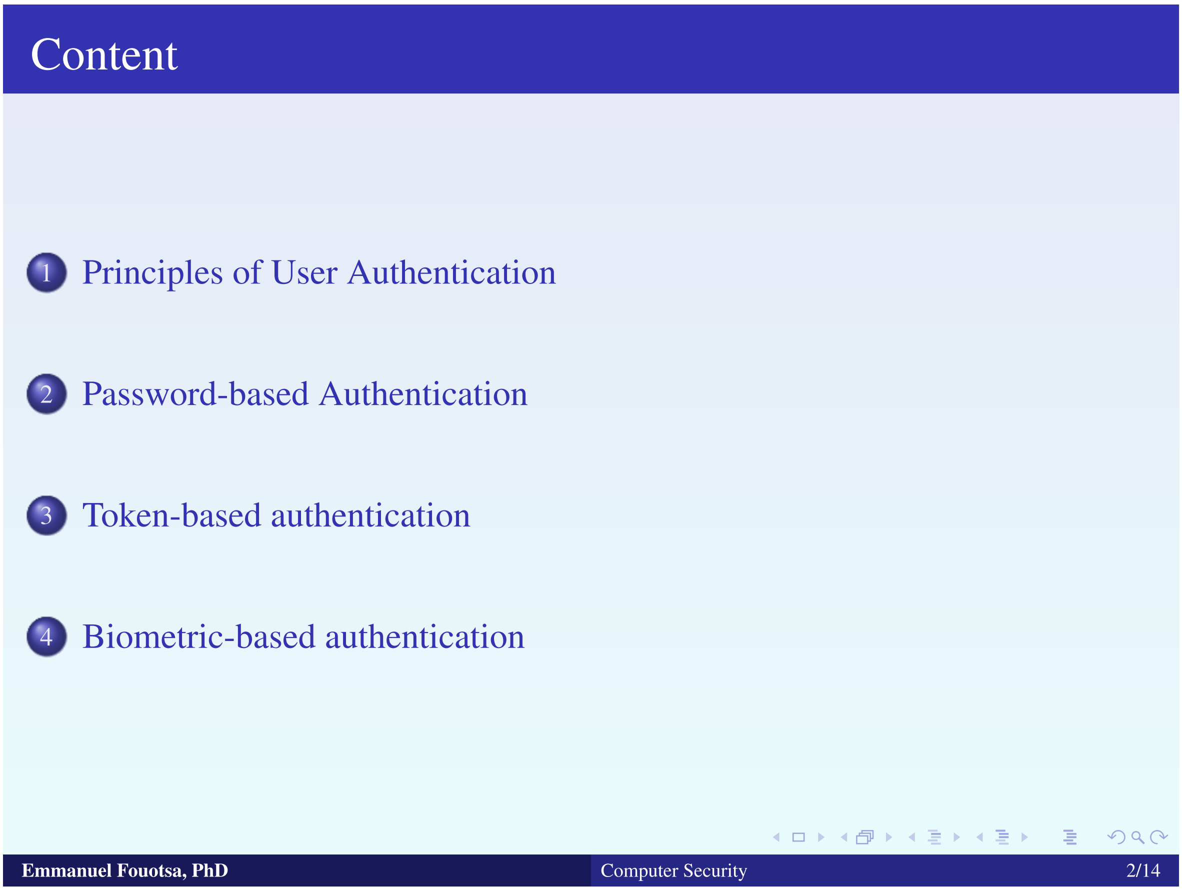


CENP 3203: Data Security and Integrity
Chapter 2: Authentication

By: Emmanuel FOUOTSA, PhD

The University of Bamenda, Cameroon
College of Technology, Bambili
Departement of Computer Engineering

April 13, 2023



Content

1. Principles of User Authentication
2. Password-based Authentication
3. Token-based authentication
4. Biometric-based authentication

Principle of User Authentication

Electronic User Authentication (NIST)

Electronic user authentication is the process of establishing confidence in user identities that are presented electronically to an information system. Systems can use the authenticated identity to determine if the authenticated individual is authorized to perform particular functions, such as database transactions or access to system resources. In many cases, the authentication and transaction or other authorized function take place across an open network such as the Internet or locally

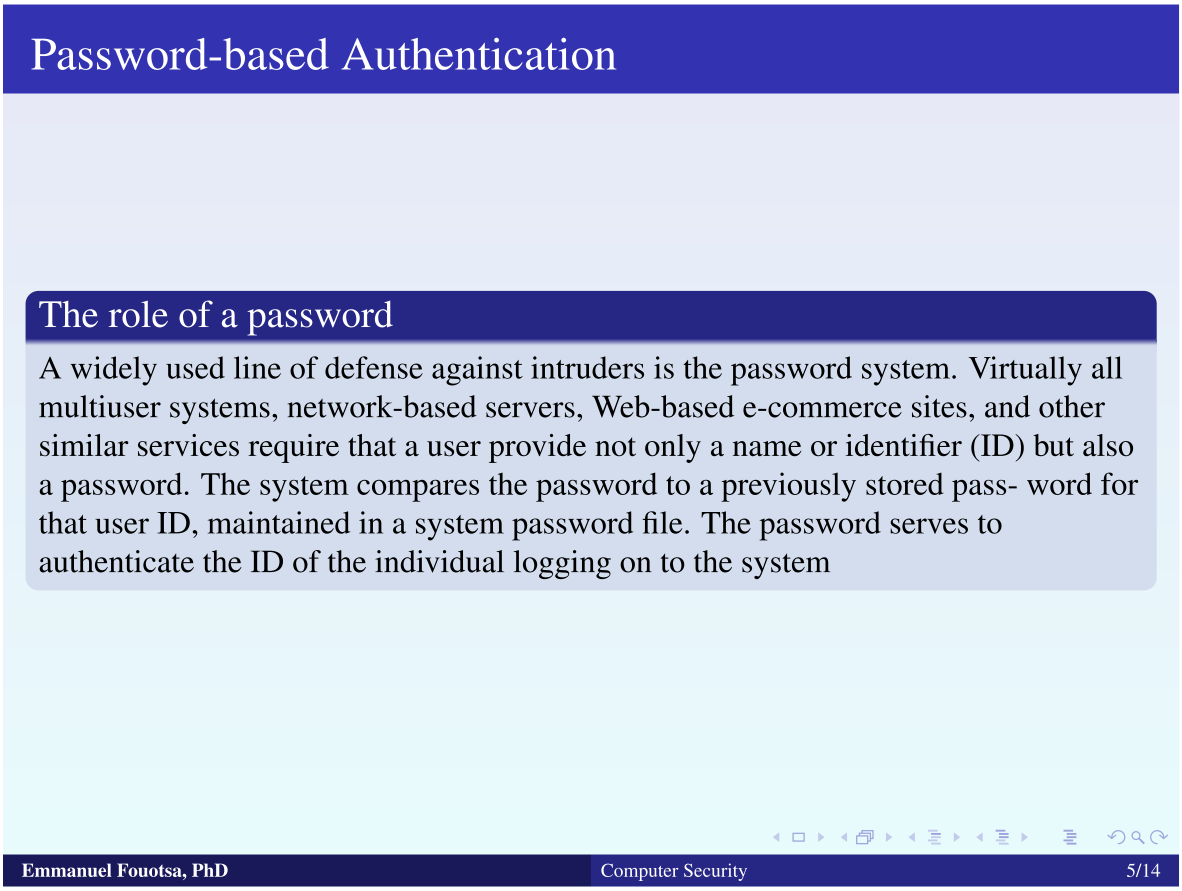
There are four general means of authenticating a user's identity, which can be used alone or in combination: what the user knows, possesses, is, or does

NIST: National Institute of Standards and Technology. NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government and private sector but has a worldwide impact.

Principles of User Authentication: Cont.

Means of Authentication

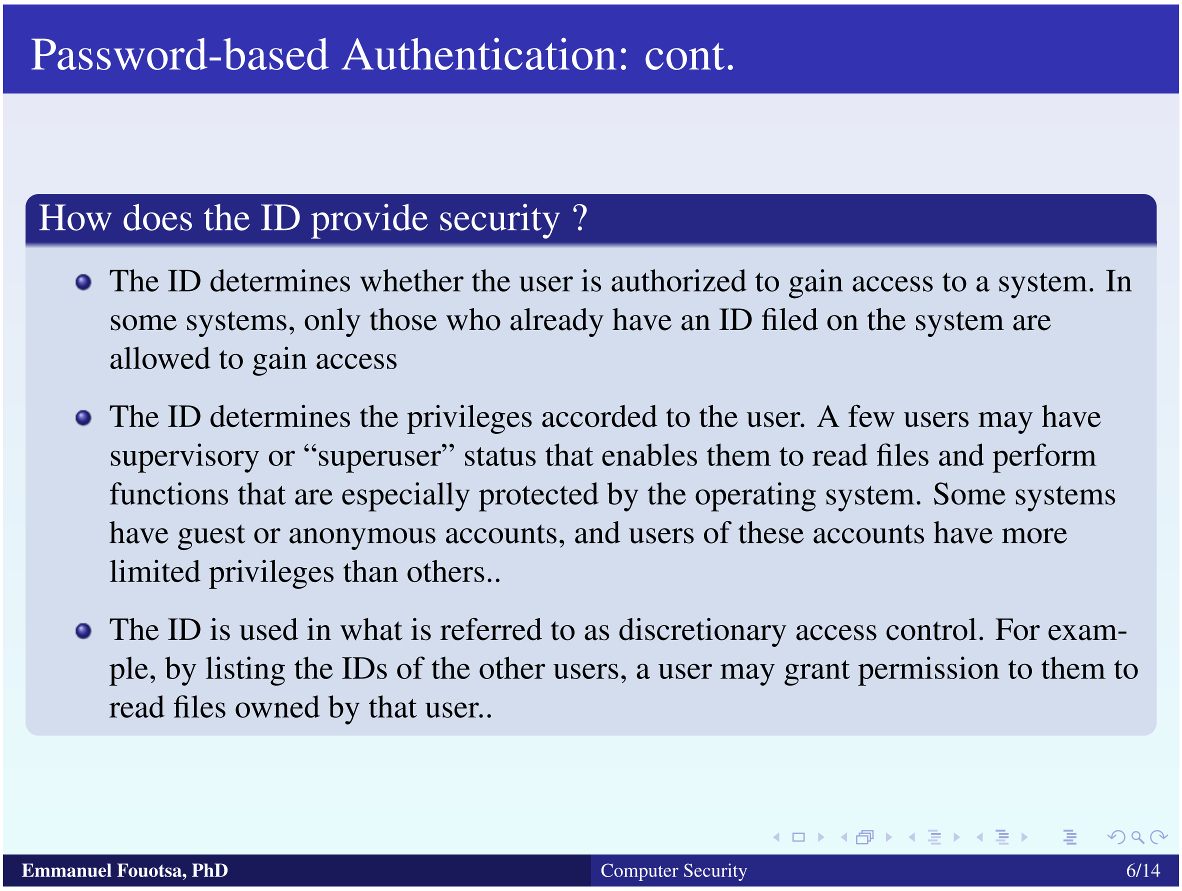
- **Something the individual knows:** Examples includes a password, a personal identification number (PIN), or answers to a prearranged set of questions.
- **Something the individual possesses:** Examples include electronic keycards, smart cards, and physical keys. This type of authenticator is referred to as a token.
- **Something the individual is (static biometrics):** Examples include recognition by fingerprint, retina, and face.
- **Something the individual does (dynamic biometrics):** Examples include recog- nition by voice pattern, handwriting characteristics, and typing rhythm.



Password-based Authentication

The role of a password

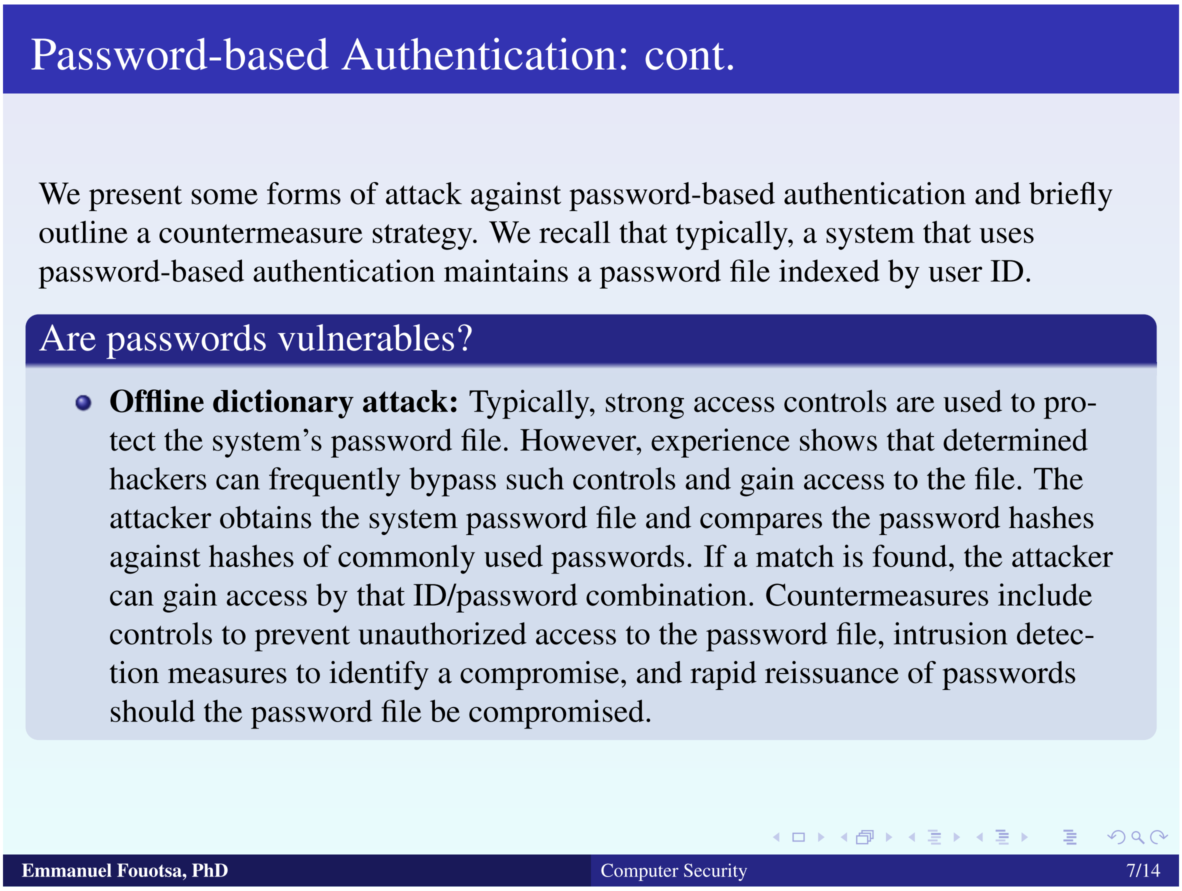
A widely used line of defense against intruders is the password system. Virtually all multiuser systems, network-based servers, Web-based e-commerce sites, and other similar services require that a user provide not only a name or identifier (ID) but also a password. The system compares the password to a previously stored pass- word for that user ID, maintained in a system password file. The password serves to authenticate the ID of the individual logging on to the system



Password-based Authentication: cont.

How does the ID provide security ?

- The ID determines whether the user is authorized to gain access to a system. In some systems, only those who already have an ID filed on the system are allowed to gain access
- The ID determines the privileges accorded to the user. A few users may have supervisory or “superuser” status that enables them to read files and perform functions that are especially protected by the operating system. Some systems have guest or anonymous accounts, and users of these accounts have more limited privileges than others..
- The ID is used in what is referred to as discretionary access control. For example, by listing the IDs of the other users, a user may grant permission to them to read files owned by that user..



Password-based Authentication: cont.

We present some forms of attack against password-based authentication and briefly outline a countermeasure strategy. We recall that typically, a system that uses password-based authentication maintains a password file indexed by user ID.

Are passwords vulnerables?

- **Offline dictionary attack:** Typically, strong access controls are used to protect the system's password file. However, experience shows that determined hackers can frequently bypass such controls and gain access to the file. The attacker obtains the system password file and compares the password hashes against hashes of commonly used passwords. If a match is found, the attacker can gain access by that ID/password combination. Countermeasures include controls to prevent unauthorized access to the password file, intrusion detection measures to identify a compromise, and rapid reissuance of passwords should the password file be compromised.

Password-based Authentication: cont.

Are passwords vulnerables? Cont.

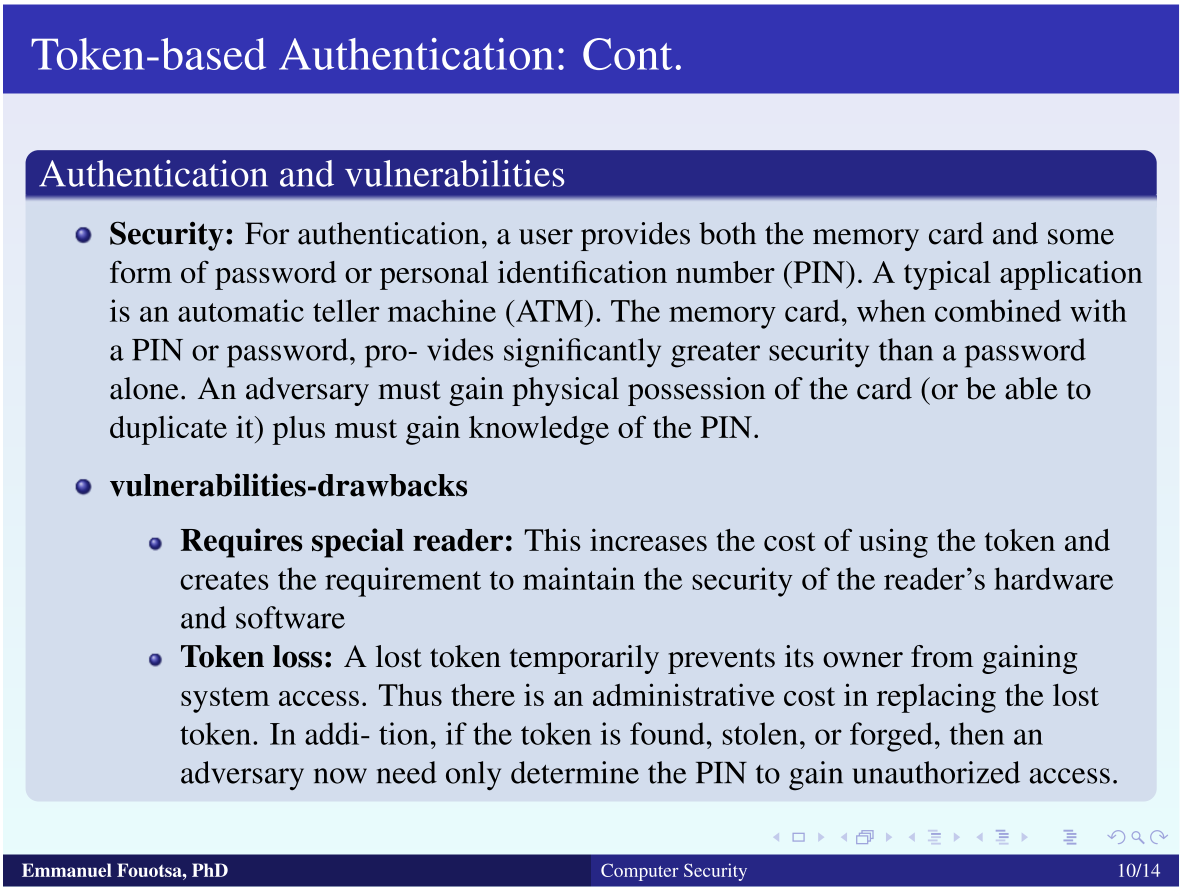
- **Specific account attack:** The attacker targets a specific account and submits password guesses until the correct password is discovered. The standard countermeasure is an account lockout mechanism, which locks out access to the account after a number of failed login attempts. Typical practice is no more than five access attempts.
- **Password guessing against single user:** The attacker attempts to gain knowledge about the account holder and system password policies and uses that knowledge to guess the password. Countermeasures include training in and enforcement of password policies that make passwords difficult to guess. Such policies address the secrecy, minimum length of the password, character set, prohibition against using well-known user identifiers, and length of time before the password must be changed.

Other attacks include: Popular password attack, Workstation hijacking, Exploiting user mistakes, Exploiting multiple password use, electronic monitoring...

Token-based Authentication

what is a token?

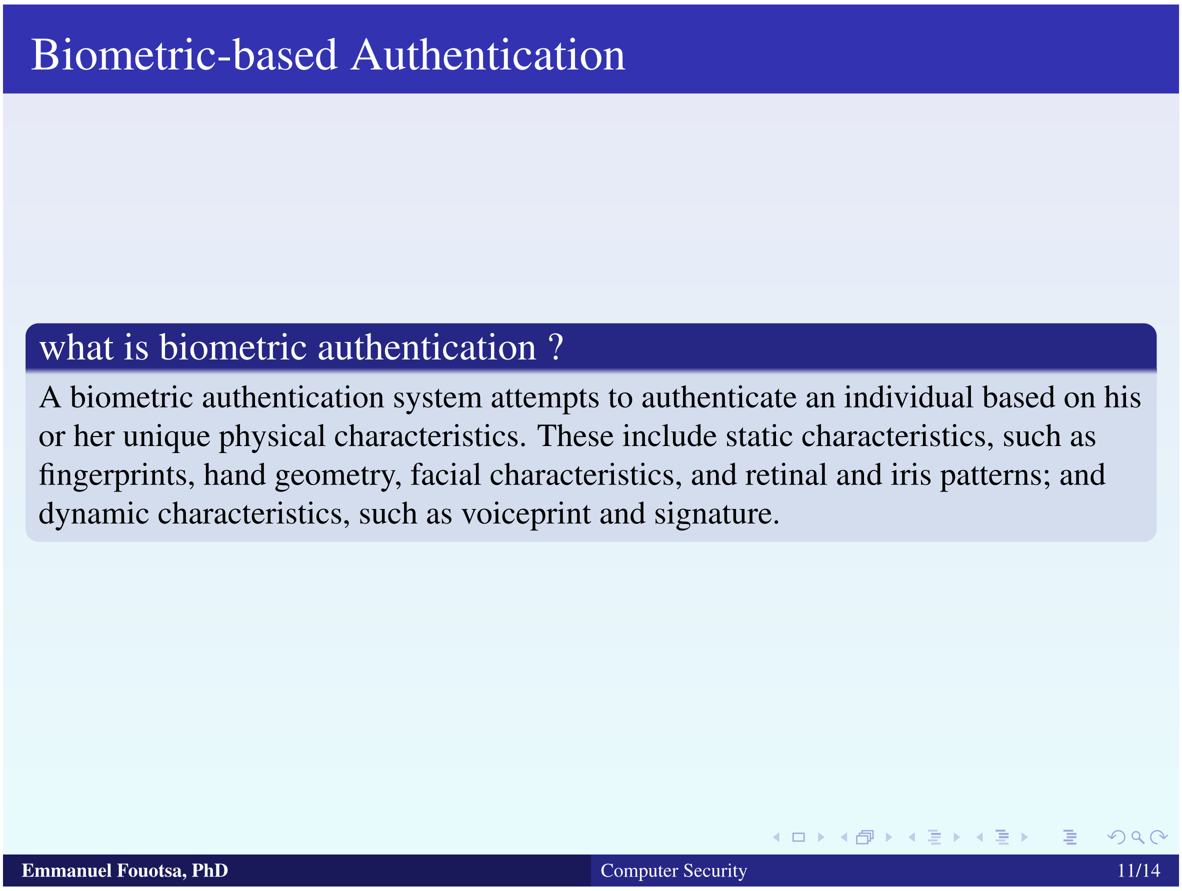
Objects that a user possesses for the purpose of user authentication are called tokens: e.g.: smart cards



Token-based Authentication: Cont.

Authentication and vulnerabilities

- **Security:** For authentication, a user provides both the memory card and some form of password or personal identification number (PIN). A typical application is an automatic teller machine (ATM). The memory card, when combined with a PIN or password, pro- vides significantly greater security than a password alone. An adversary must gain physical possession of the card (or be able to duplicate it) plus must gain knowledge of the PIN.
- **vulnerabilities-drawbacks**
  - **Requires special reader:** This increases the cost of using the token and creates the requirement to maintain the security of the reader's hardware and software
  - **Token loss:** A lost token temporarily prevents its owner from gaining system access. Thus there is an administrative cost in replacing the lost token. In addi- tion, if the token is found, stolen, or forged, then an adversary now need only determine the PIN to gain unauthorized access.



Biometric-based Authentication

what is biometric authentication ?

A biometric authentication system attempts to authenticate an individual based on his or her unique physical characteristics. These include static characteristics, such as fingerprints, hand geometry, facial characteristics, and retinal and iris patterns; and dynamic characteristics, such as voiceprint and signature.

Biometric-based Authentication: cont.

Biometric enrollement 1

- Each individual who is to be included in the database of authorized users must first be enrolled in the system. This is analogous to assigning a password to a user. For a biometric system, the user presents a name and, typically, some type of password or PIN to the system. At the same time the system senses some biometric characteristic of this user (e.g., finger- print of right index finger). The system digitizes the input and then extracts a set of features that can be stored as a number or set of numbers representing this unique biometric characteristic; this set of numbers is referred to as the user's template. The user is now enrolled in the system, which maintains for the user a name (ID), perhaps a PIN or password, and the biometric value.
- Depending on application, user authentication on a biometric system involves either verification or identification. For biometric verification, the user enters a PIN and also uses a biometric sensor. The system extracts the corresponding feature and compares that to the template stored for this user. If there is a match, then the system authenticates this user. For an identification system, the individual uses the biometric sensor but presents no additional information. The system then compares the presented template with the set of stored templates. If there is a match, then this user is identified. Otherwise, the user is rejected.

Biometric-based Authentication: cont.

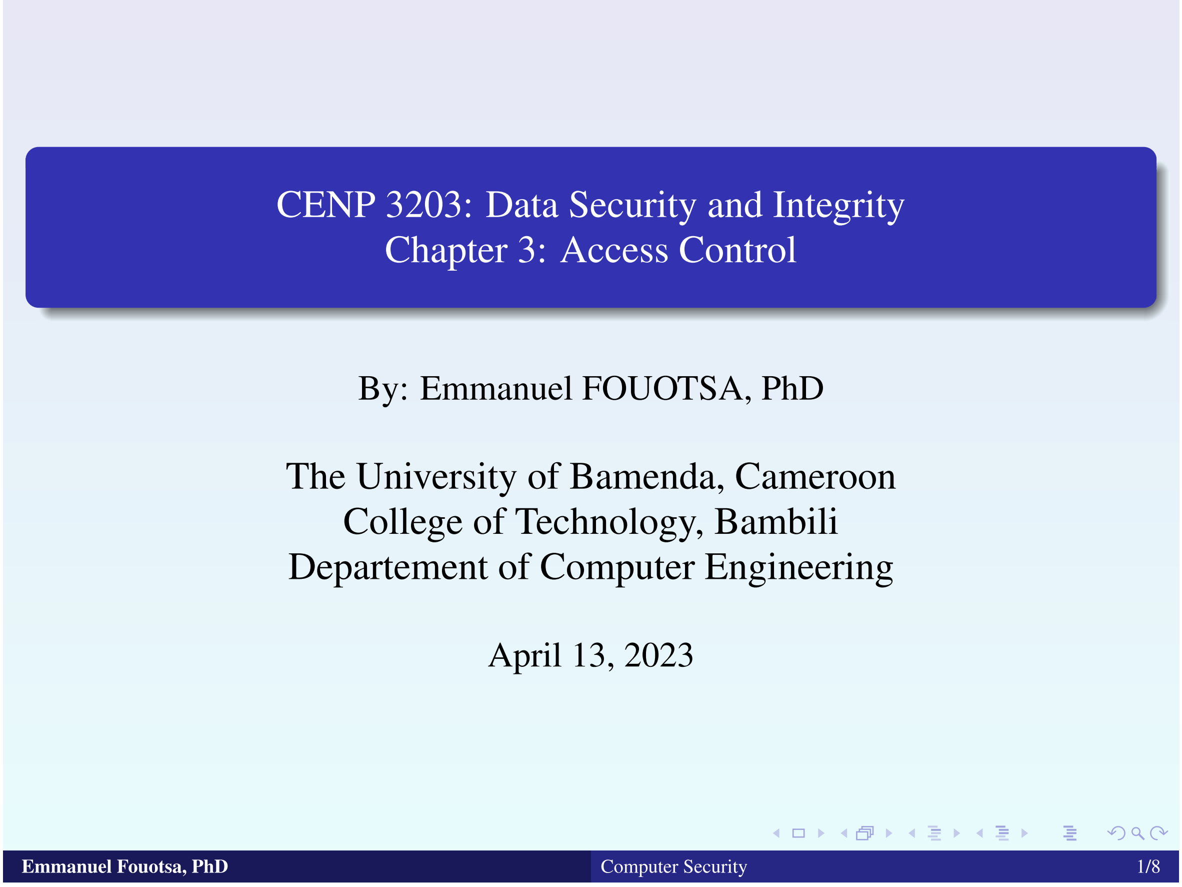
Biometric enrollement 1

- Each individual who is to be included in the database of authorized users must first be enrolled in the system. This is analogous to assigning a password to a user. For a biometric system, the user presents a name and, typically, some type of password or PIN to the system. At the same time the system senses some biometric characteristic of this user (e.g., finger- print of right index finger). The system digitizes the input and then extracts a set of features that can be stored as a number or set of numbers representing this unique biometric characteristic; this set of numbers is referred to as the user's template. The user is now enrolled in the system, which maintains for the user a name (ID), perhaps a PIN or password, and the biometric value.

Biometric-based Authentication: cont.

Biometric Authentication 2

- Depending on application, user authentication on a biometric system involves either verification or identification.
  - For biometric verification, the user enters a PIN and also uses a biometric sensor. The system extracts the corresponding feature and compares that to the template stored for this user. If there is a match, then the system authenticates this user.
  - For an identification system, the individual uses the biometric sensor but presents no additional information. The system then compares the presented template with the set of stored templates. If there is a match, then this user is identified. Otherwise, the user is rejected.



CENP 3203: Data Security and Integrity
Chapter 3: Access Control

By: Emmanuel FOUOTSA, PhD

The University of Bamenda, Cameroon
College of Technology, Bambili
Departement of Computer Engineering

April 13, 2023

Content

1. Principles of Access Control
2. Some key terms in Access Control
3. Access Control Policies
4. Examples and Projects

definitions of Access Control

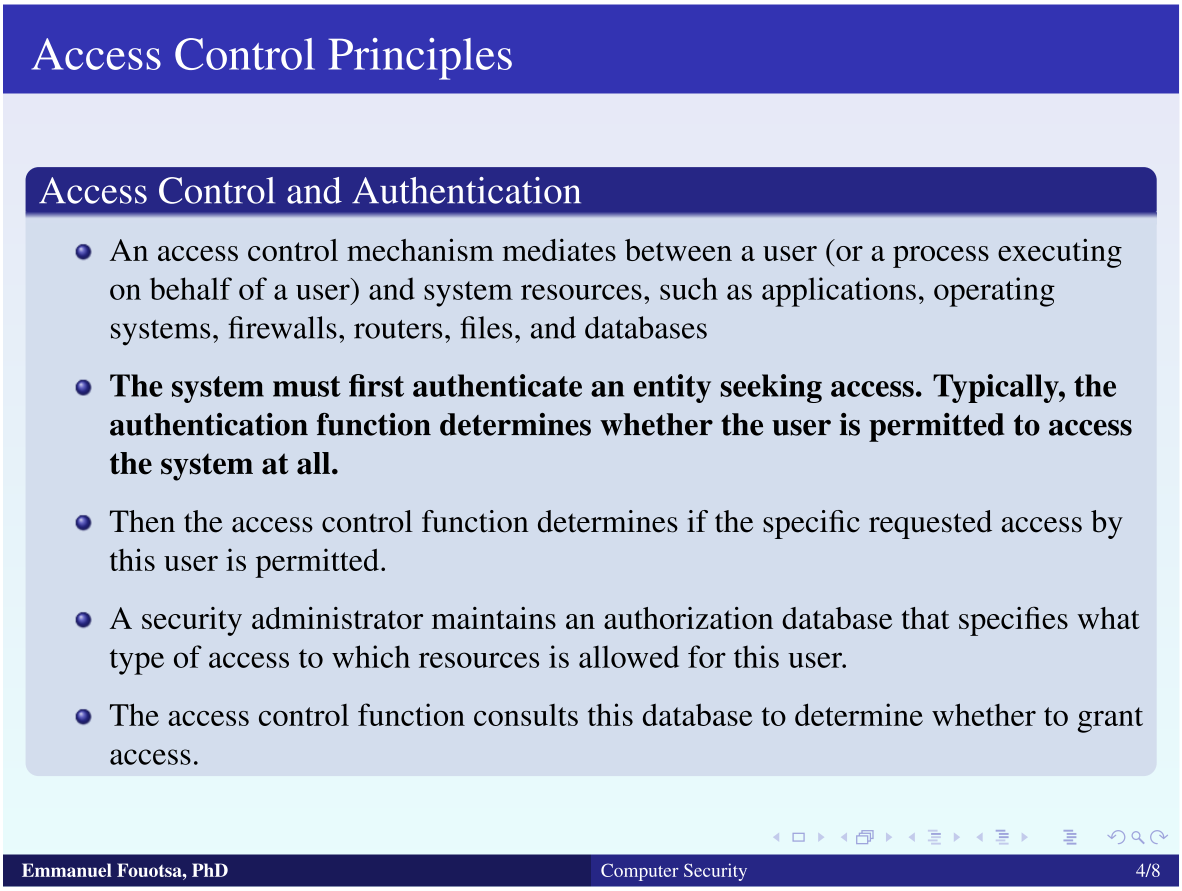
Access Control (NIST)

Access Control as the process of granting or denying specific requests to: (1) obtain and use information and related information processing services; and (2) enter specific physical facilities

Access Control (Internet Security Glossary)

Access Control as a process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy.

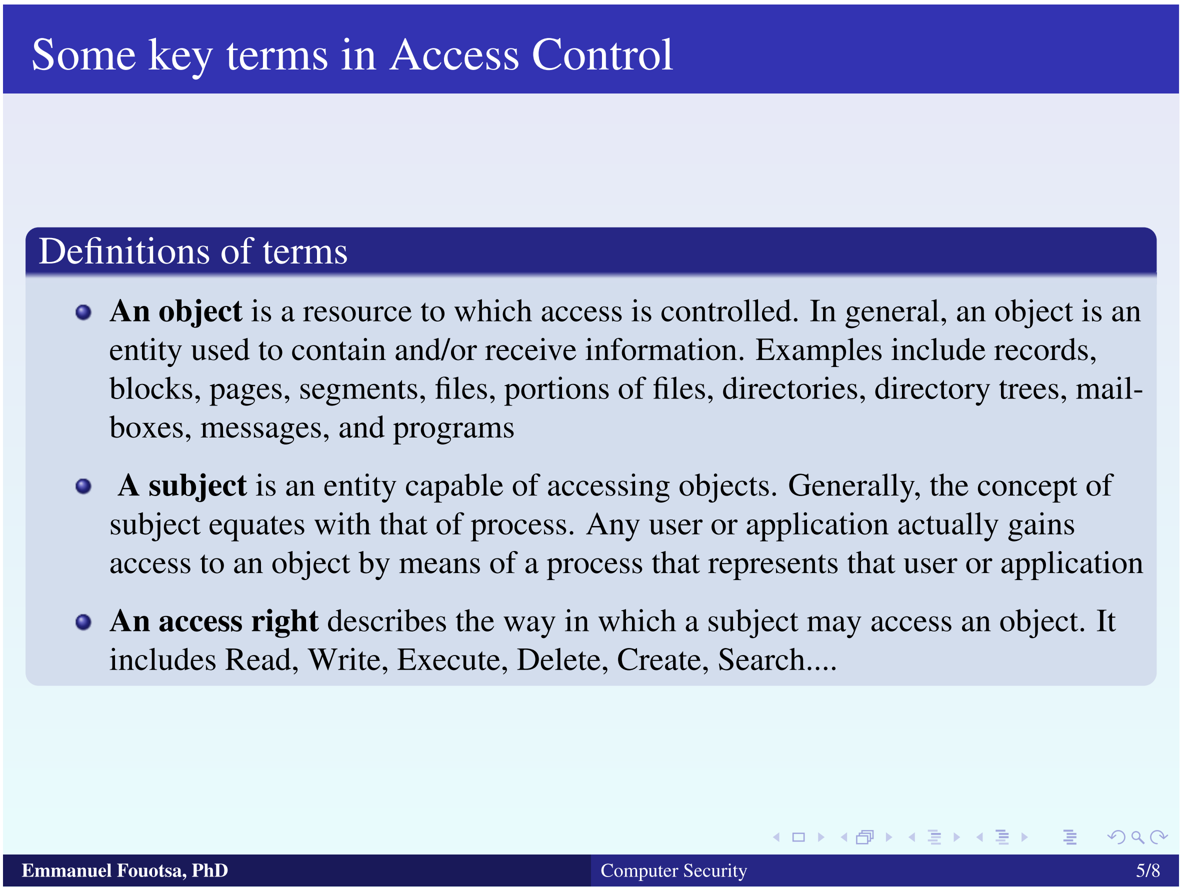
We can view access control as the central element of computer security. The principal objectives of computer security are to prevent unauthorized users from gaining access to resources, to prevent legitimate users from accessing resources in an unauthorized manner, and to enable legitimate users to access resources in an authorized manner



Access Control Principles

Access Control and Authentication

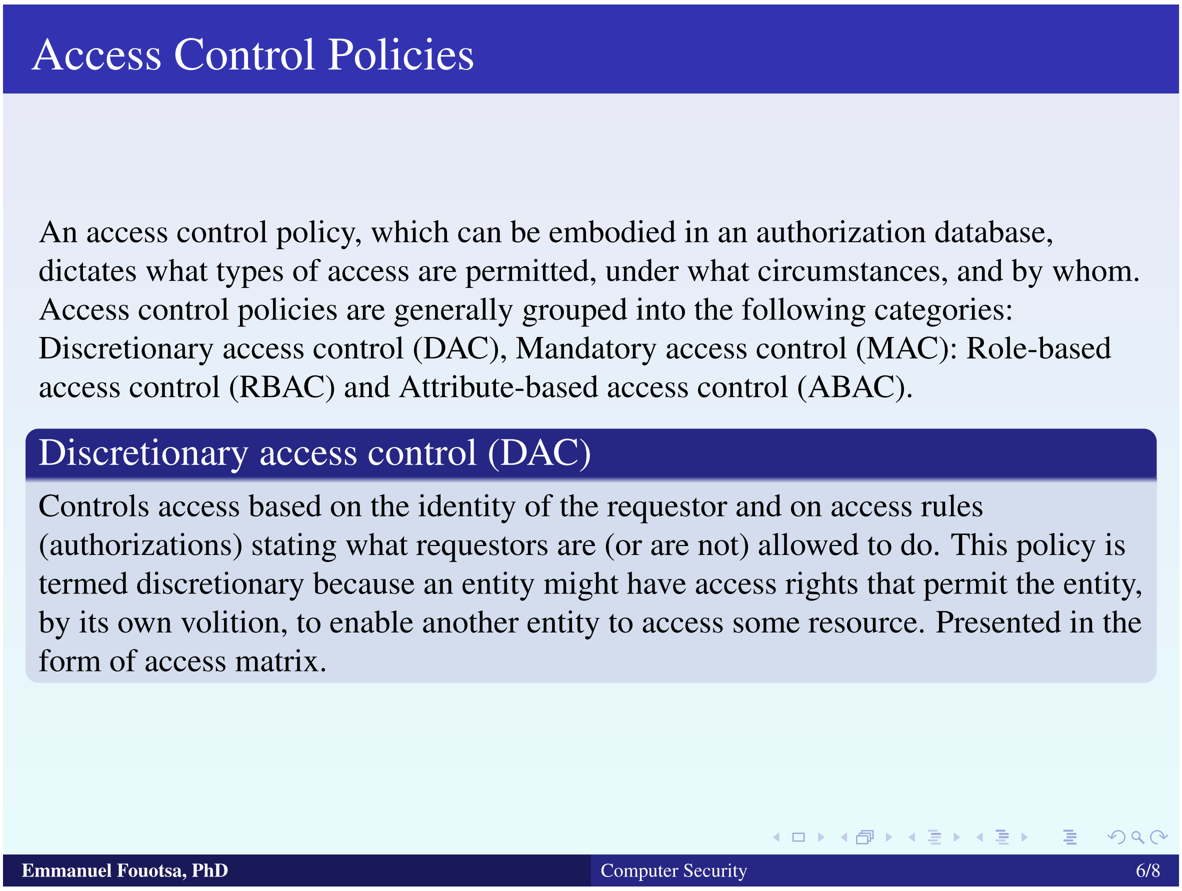
- An access control mechanism mediates between a user (or a process executing on behalf of a user) and system resources, such as applications, operating systems, firewalls, routers, files, and databases
- **The system must first authenticate an entity seeking access. Typically, the authentication function determines whether the user is permitted to access the system at all.**
- Then the access control function determines if the specific requested access by this user is permitted.
- A security administrator maintains an authorization database that specifies what type of access to which resources is allowed for this user.
- The access control function consults this database to determine whether to grant access.



Some key terms in Access Control

Definitions of terms

- **An object** is a resource to which access is controlled. In general, an object is an entity used to contain and/or receive information. Examples include records, blocks, pages, segments, files, portions of files, directories, directory trees, mailboxes, messages, and programs
- **A subject** is an entity capable of accessing objects. Generally, the concept of subject equates with that of process. Any user or application actually gains access to an object by means of a process that represents that user or application
- **An access right** describes the way in which a subject may access an object. It includes Read, Write, Execute, Delete, Create, Search....

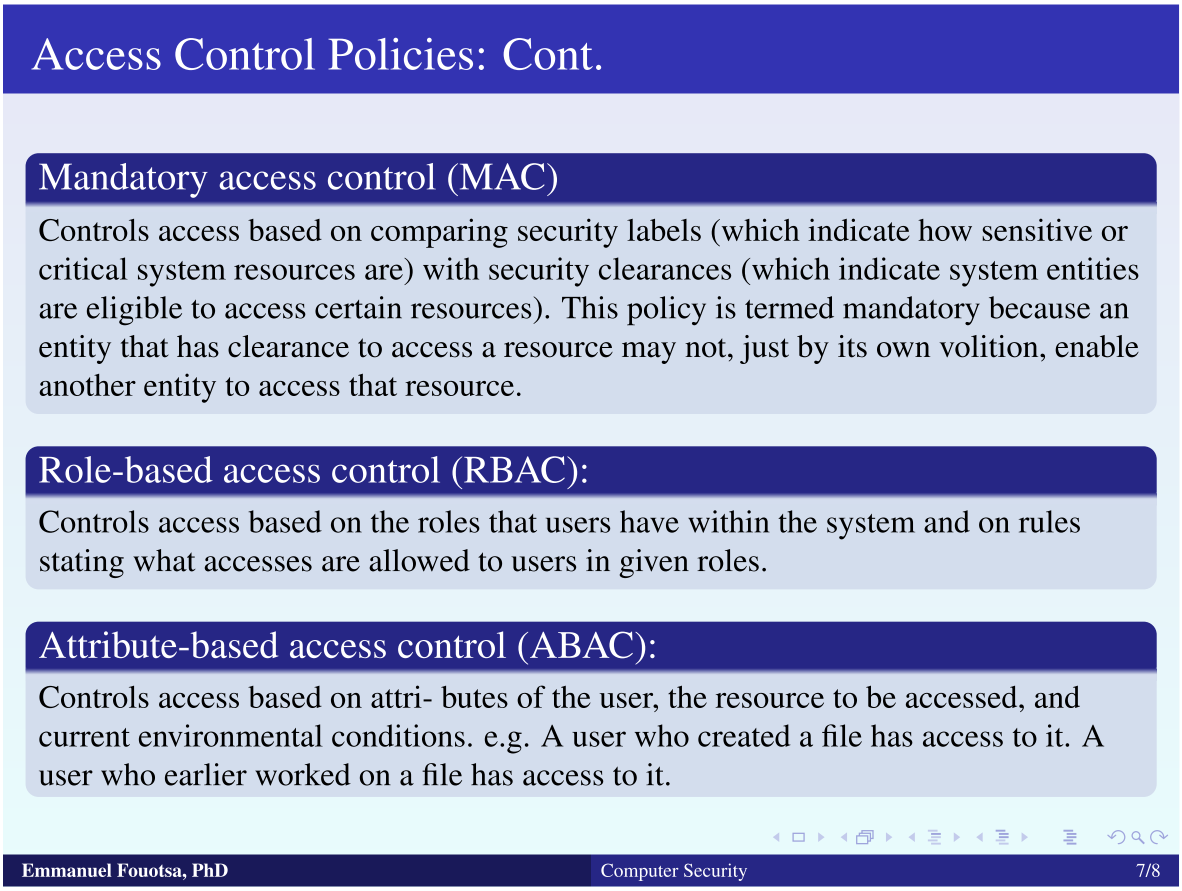


Access Control Policies

An access control policy, which can be embodied in an authorization database, dictates what types of access are permitted, under what circumstances, and by whom. Access control policies are generally grouped into the following categories: Discretionary access control (DAC), Mandatory access control (MAC): Role-based access control (RBAC) and Attribute-based access control (ABAC).

Discretionary access control (DAC)

Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do. This policy is termed discretionary because an entity might have access rights that permit the entity, by its own volition, to enable another entity to access some resource. Presented in the form of access matrix.



Access Control Policies: Cont.

Mandatory access control (MAC)

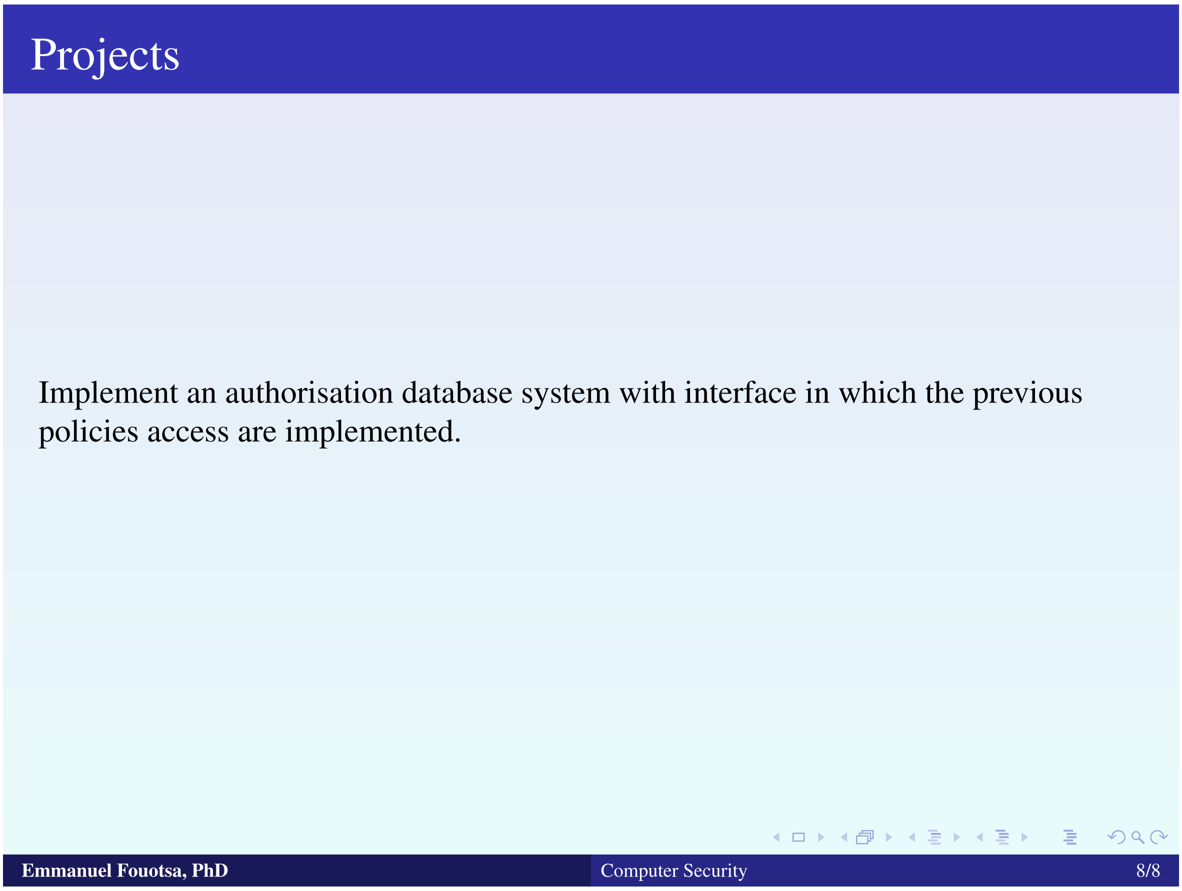
Controls access based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources). This policy is termed mandatory because an entity that has clearance to access a resource may not, just by its own volition, enable another entity to access that resource.

Role-based access control (RBAC):

Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

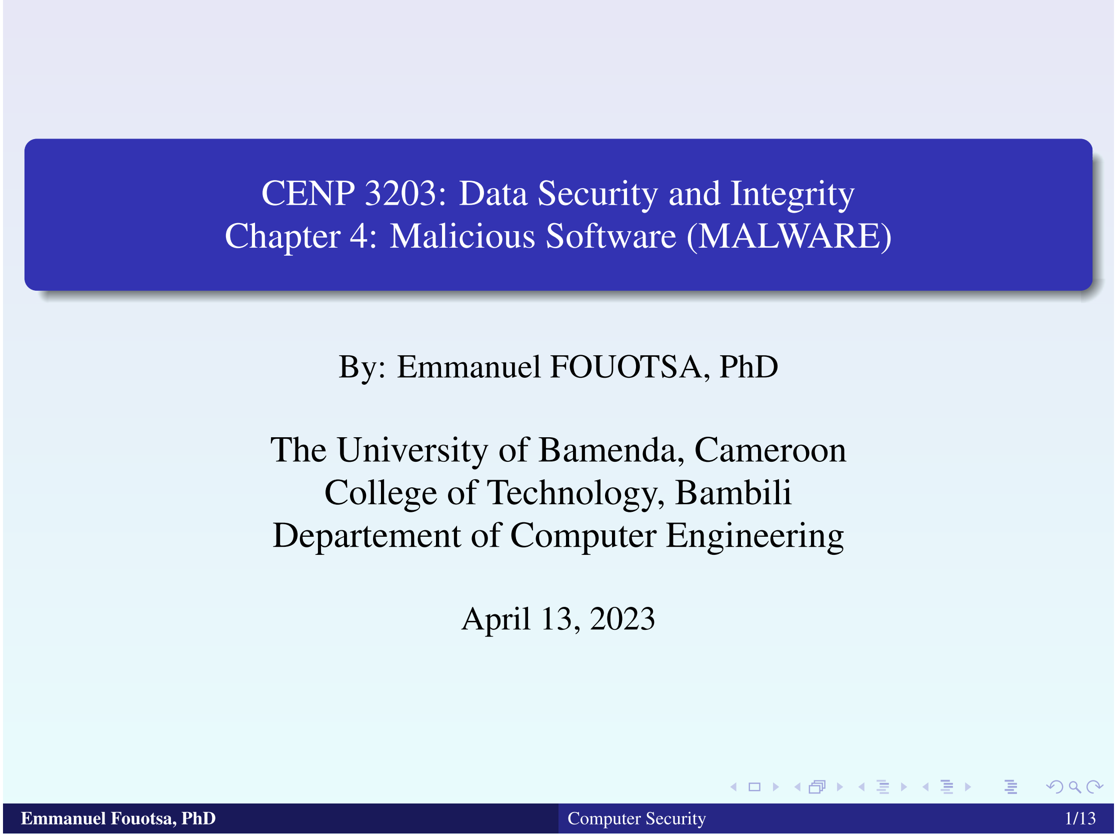
Attribute-based access control (ABAC):

Controls access based on attri- butes of the user, the resource to be accessed, and current environmental conditions. e.g. A user who created a file has access to it. A user who earlier worked on a file has access to it.



Projects

Implement an authorisation database system with interface in which the previous policies access are implemented.



CENP 3203: Data Security and Integrity
Chapter 4: Malicious Software (MALWARE)

By: Emmanuel FOUOTSA, PhD

The University of Bamenda, Cameroon
College of Technology, Bambili
Departement of Computer Engineering

April 13, 2023

Content

1. Definition, objectives and types of malware

2. Propagation-Infected content malware

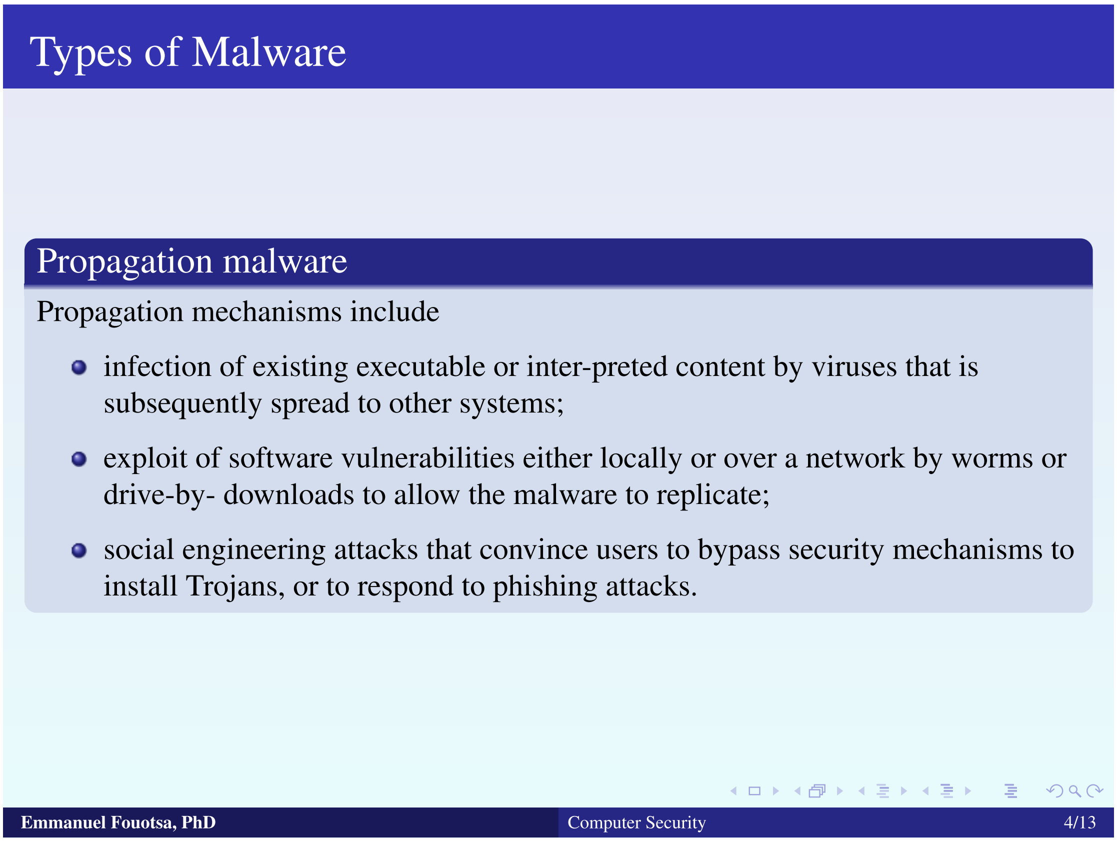
3. Malware Actions

Definition, objectives and types of malware

Malicious software, or malware, arguably constitutes one of the most significant categories of threats to computer systems. Indeed malware is defined as “a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or otherwise annoying or disrupting the victim.”

Classification of malwares

Although a range of aspects can be used, one useful approach classifies malware into two broad categories, based first on how it **spreads or propagates** to reach the desired targets; and then on the **actions or payloads** it performs once a target is reached.



Types of Malware

Propagation malware

Propagation mechanisms include

- infection of existing executable or inter-preted content by viruses that is subsequently spread to other systems;
- exploit of software vulnerabilities either locally or over a network by worms or drive-by- downloads to allow the malware to replicate;
- social engineering attacks that convince users to bypass security mechanisms to install Trojans, or to respond to phishing attacks.

Types of Malware

Payload malware (malware d'actions)

Payload actions performed by malware once it reaches a target system can include

- icorruption of system or data files; theft of service in order to make the system a zombie agent of attack as part of a botnet;
- theft of information from the system, especially of logins, passwords, or other personal details by keylogging or spyware programs;
- stealthing where the malware hides its presence on the system from attempts to detect and block it.

Definition of a crimeware

A crimeware is a toolkit for viruses (malware) creation/developpement. e.g.: the Zeus crimeware toolkit, the Blackhole Sakura and Phoenix crimware.

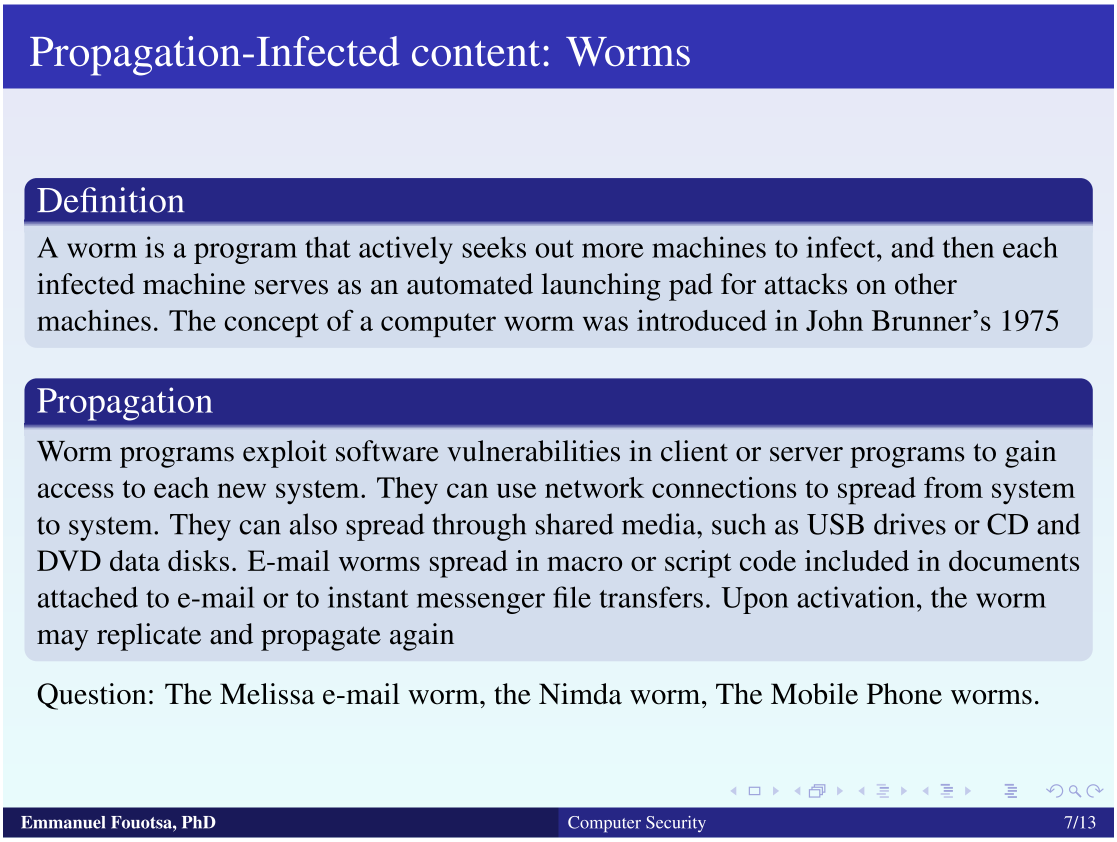
Propagation-Infected content: Viruses

Definition

computer virus is a piece of software that can “infect” other programs, or indeed any type of executable content, by modifying them. Computer viruses first appeared in the early 1980s, and the term itself is attributed to Fred Cohen.

Propagation

a computer virus carries in its instructional code the recipe for making perfect copies of itself. The typical virus becomes embedded in a program, or carrier of executable content, on a computer. Then, whenever the infected computer comes into contact with an uninfected piece of code, a fresh copy of the virus passes into the new location. Thus, the infection can spread from computer to computer, aided by unsuspecting users, who exchange these programs or carrier files on disk or USB stick; or who send them to one another over a network. In a network environment, the ability to access documents, applications, and system services on other computers provides a perfect culture for the spread of such viral code.



Propagation-Infected content: Worms

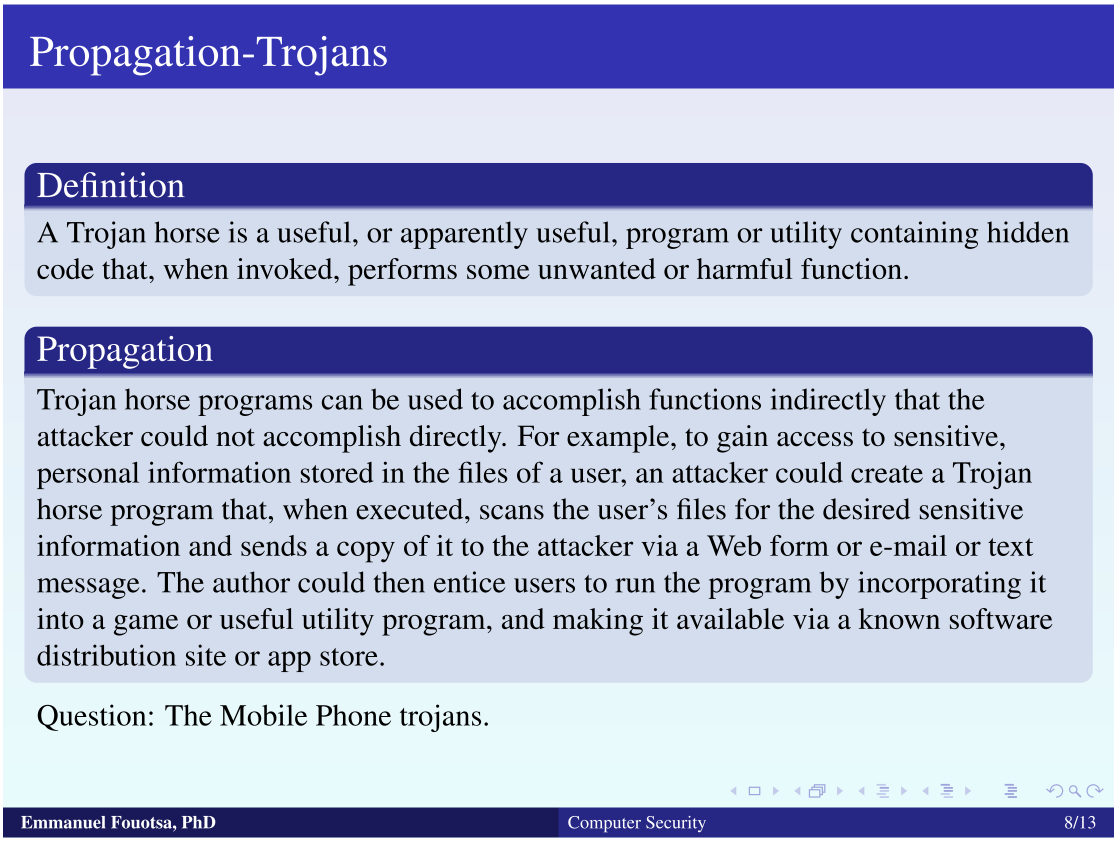
Definition

A worm is a program that actively seeks out more machines to infect, and then each infected machine serves as an automated launching pad for attacks on other machines. The concept of a computer worm was introduced in John Brunner's 1975

Propagation

Worm programs exploit software vulnerabilities in client or server programs to gain access to each new system. They can use network connections to spread from system to system. They can also spread through shared media, such as USB drives or CD and DVD data disks. E-mail worms spread in macro or script code included in documents attached to e-mail or to instant messenger file transfers. Upon activation, the worm may replicate and propagate again

Question: The Melissa e-mail worm, the Nimda worm, The Mobile Phone worms.



Propagation-Trojans

Definition

A Trojan horse is a useful, or apparently useful, program or utility containing hidden code that, when invoked, performs some unwanted or harmful function.

Propagation

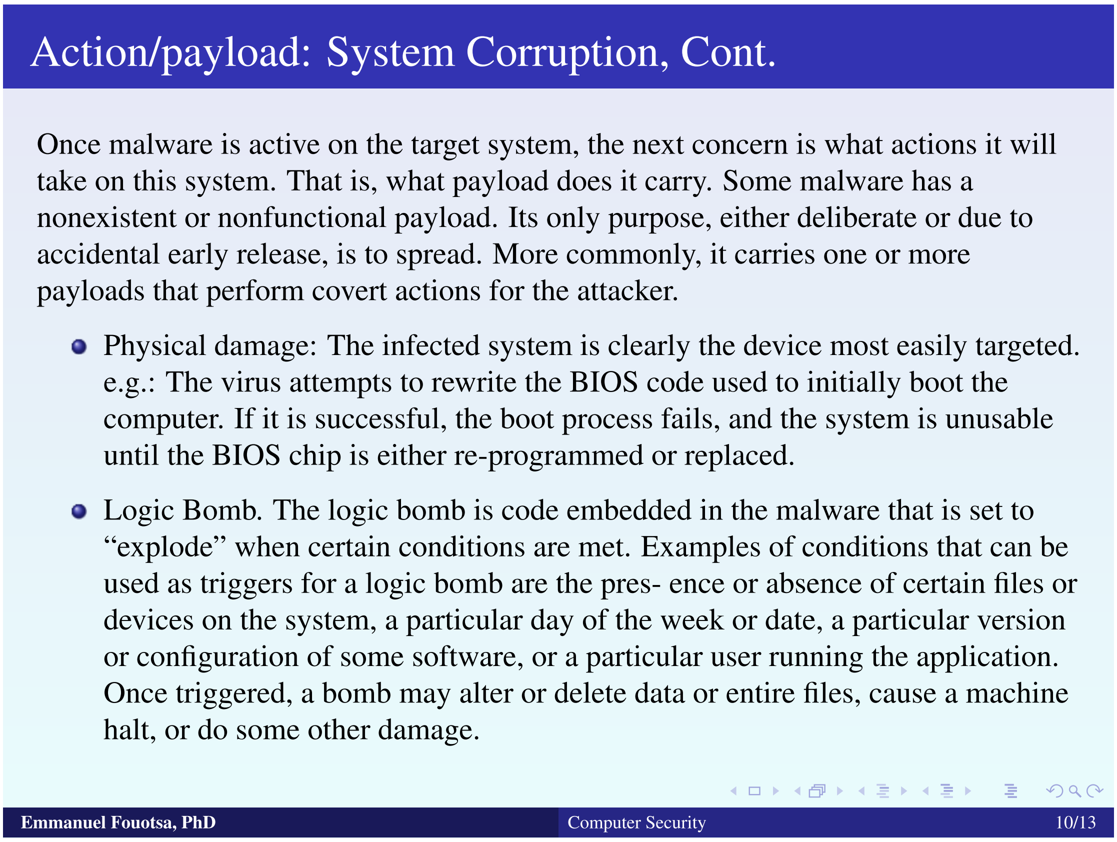
Trojan horse programs can be used to accomplish functions indirectly that the attacker could not accomplish directly. For example, to gain access to sensitive, personal information stored in the files of a user, an attacker could create a Trojan horse program that, when executed, scans the user's files for the desired sensitive information and sends a copy of it to the attacker via a Web form or e-mail or text message. The author could then entice users to run the program by incorporating it into a game or useful utility program, and making it available via a known software distribution site or app store.

Question: The Mobile Phone trojans.

Action/payload: System Corruption

Once malware is active on the target system, the next concern is what actions it will take on this system. That is, what payload does it carry. Some malware has a nonexistent or nonfunctional payload. Its only purpose, either deliberate or due to accidental early release, is to spread. More commonly, it carries one or more payloads that perform covert actions for the attacker.

- Data Destruction. e.g.: The Chernobyl virus is an early example of a destructive parasitic memory-resident Windows-95 and 98 virus, that was first seen in 1998. It infects executable files when they are opened. And when a trigger date is reached, it deletes data on the infected system by overwriting the first megabyte of the hard drive with zeroes, resulting in massive corruption of the entire file system. This first occurred on April 26, 1999, when estimates suggest more than one million computers were affected.
- Data Encryption. As an alternative to just destroying data, some malware encrypts the user's data, and demands payment in order to access the key needed to recover this information. This is sometimes known as **ransomware**.e.g.: The Gpcode Trojan.



Action/payload: System Corruption, Cont.

Once malware is active on the target system, the next concern is what actions it will take on this system. That is, what payload does it carry. Some malware has a nonexistent or nonfunctional payload. Its only purpose, either deliberate or due to accidental early release, is to spread. More commonly, it carries one or more payloads that perform covert actions for the attacker.

- Physical damage: The infected system is clearly the device most easily targeted. e.g.: The virus attempts to rewrite the BIOS code used to initially boot the computer. If it is successful, the boot process fails, and the system is unusable until the BIOS chip is either re-programmed or replaced.
- Logic Bomb. The logic bomb is code embedded in the malware that is set to “explode” when certain conditions are met. Examples of conditions that can be used as triggers for a logic bomb are the pres- ence or absence of certain files or devices on the system, a particular day of the week or date, a particular version or configuration of some software, or a particular user running the application. Once triggered, a bomb may alter or delete data or entire files, cause a machine halt, or do some other damage.

Action/payload: Zombie, Bots

the malware subverts the compu- tational and network resources of the infected system for use by the attacker. Such a system is known as a bot (robot), zombie or drone, and secretly takes over another Internet-attached computer and then uses that computer to launch or manage. Some of the use of bots are the following

- Spamming: With the help of a botnet and thousands of bots, an attacker is able to send massive amounts of bulk e-mail (spam).
- Sniffing traffic: Bots can also use a packet sniffer to watch for interesting clear-text data passing by a compromised machine. The sniffers are mostly used to retrieve sensitive information like usernames and passwords.
- Keylogging: If the compromised machine uses encrypted communication channels (e.g. HTTPS or POP3S), then just sniffing the network packets on the victim's computer is useless because the appropriate key to decrypt the packets is missing. But by using a keylogger, which captures keystrokes on the infected machine, an attacker can retrieve sensitive information.
- Installing advertisement add-ons and browser helper objects (BHOs): Botnets can also be used to gain financial advantages. This works by setting up a fake Web site with some advertisements: The operator of this Web site negotiates a deal with some hosting companies that pay for clicks on ads. With the help of a

Action/payload: Keyloggers, Phising, Spyware

The malware gathers data stored on the infected system for use by the attacker. A common target is the user's login and password credentials to banking, gaming, and related sites, which the attacker then uses to impersonate the user to access these sites for gain.

- Typically, users send their login and password credentials to banking, gaming, and related sites over encrypted communication channels (e.g., HTTPS or POP3S), which protects them from capture by monitoring network packets. To bypass this, an attacker can install a keylogger, which captures keystrokes on the infected machine to allow an attacker to monitor this sensitive information. Since this would result in the attacker receiving a copy of all text entered on the compromised machine, keyloggers typically implement some form of filtering mechanism that only returns information close to desired keywords (e.g., password).
  Advanced keyloggers also include monitoring the history and content of browsing activity, redirecting certain Web page requests to fake sites controlled by the attacker, and dynamically modifying data exchanged between the browser and certain Web sites of interest. All of which can result in significant compromise of the user's personal information. software for such actions are called Spyware.

Action/payload: Keyloggers, Phising, Spyware: Cont.

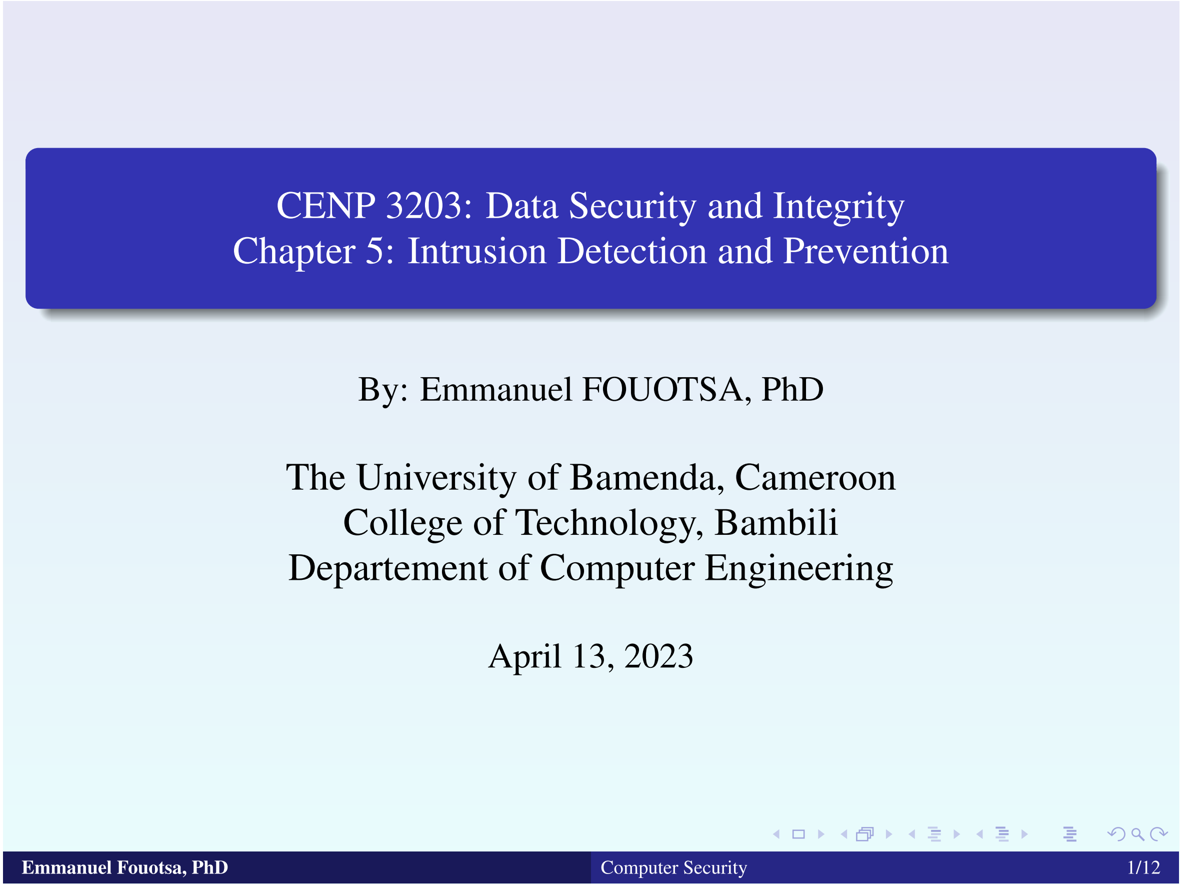
Phishing

Phishing is another approach used to capture a user's login and password credentials by including a URL in a spam e-mail that links to a fake Web site controlled by the attacker, but which mimics the login page of some banking, gaming, or similar site. This is normally included in some message suggesting that urgent action is required by the user to authenticate their account, to prevent it being locked. If the user is careless, and does not realize that they are being conned, then following the link and supplying the requested details will certainly result in the attackers exploiting their account using the captured credentials.

Blackdoor

A backdoor, also known as a trapdoor, is a secret entry point into a program that allows someone who is aware of the backdoor to gain access without going through the usual security access procedures.

Exercise: Countermeasures to the previous payloads.

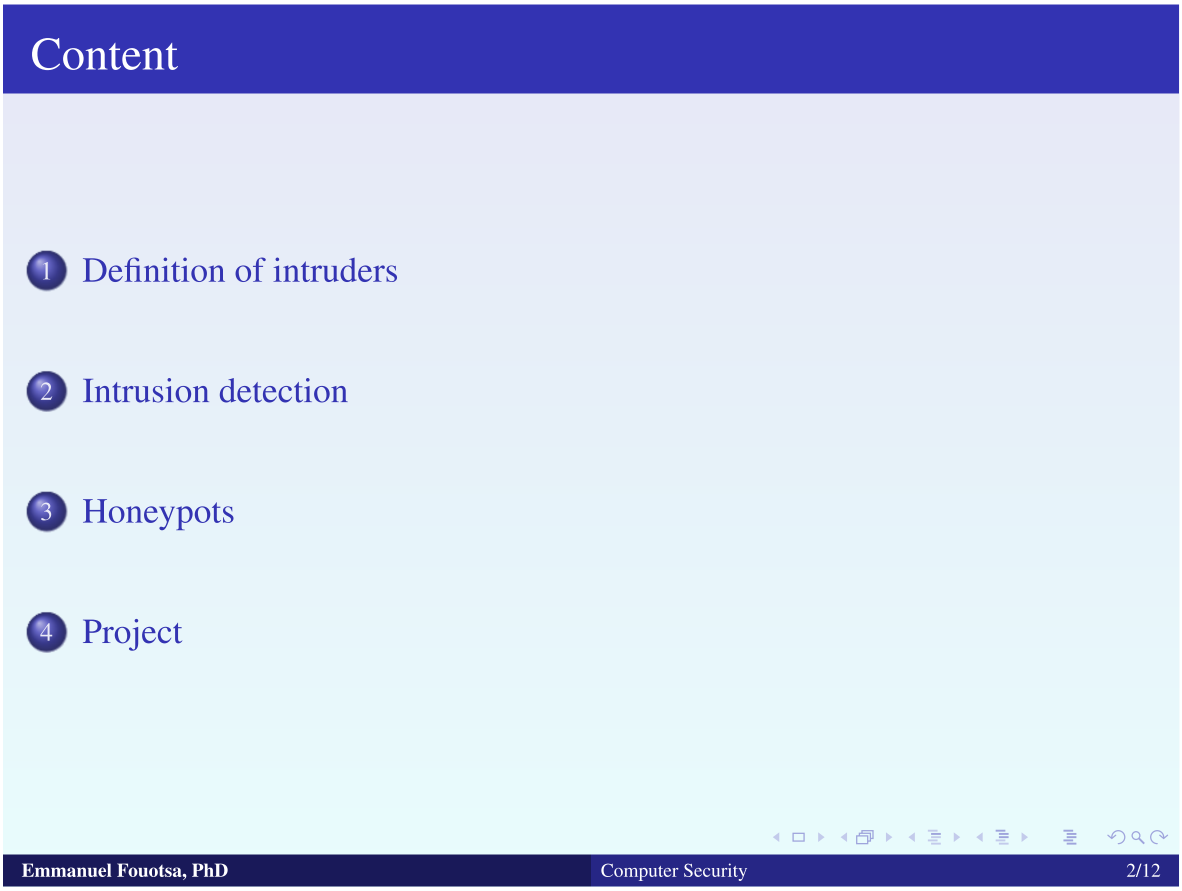


CENP 3203: Data Security and Integrity
Chapter 5: Intrusion Detection and Prevention

By: Emmanuel FOUOTSA, PhD

The University of Bamenda, Cameroon
College of Technology, Bambili
Departement of Computer Engineering

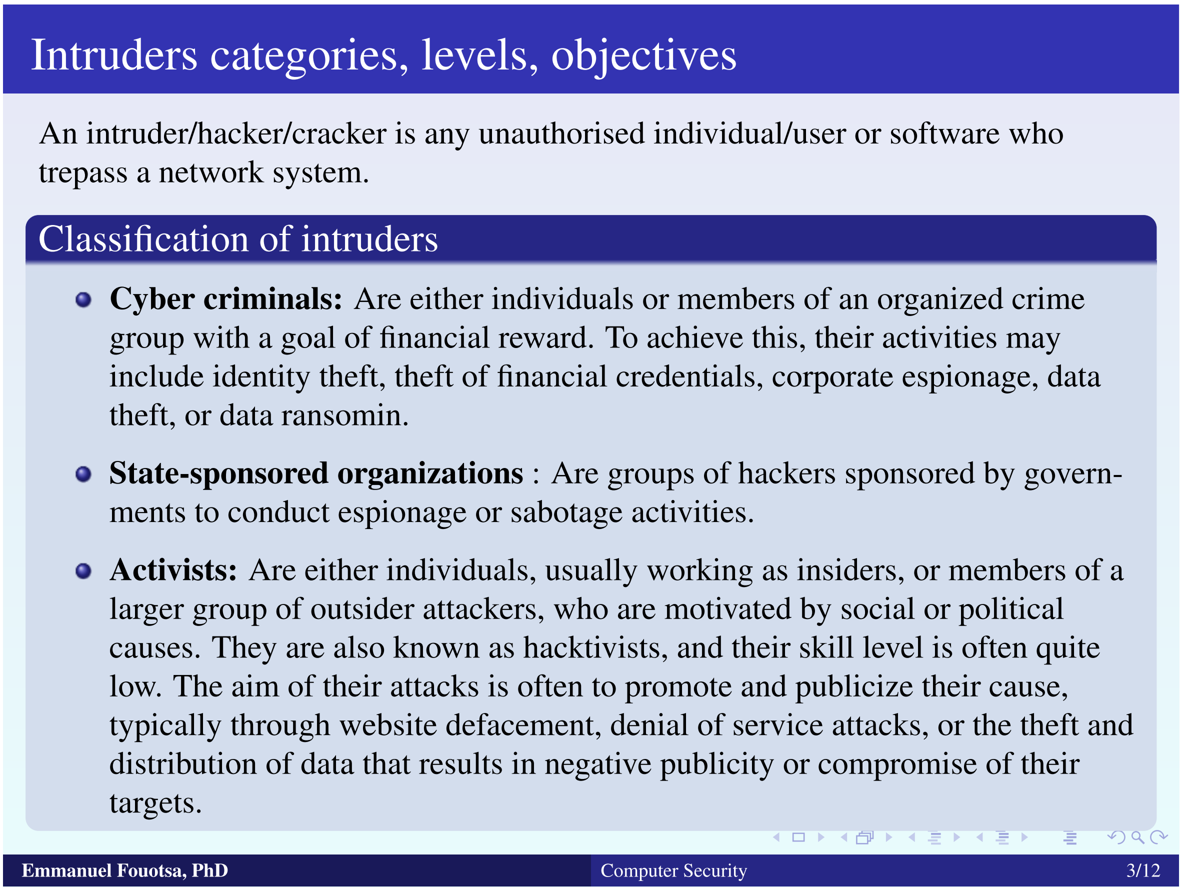
April 13, 2023



Content

1. Definition of intruders
2. Intrusion detection
3. Honeypots
4. Project

Emmanuel Fouotsa, PhD Computer Security 2/12

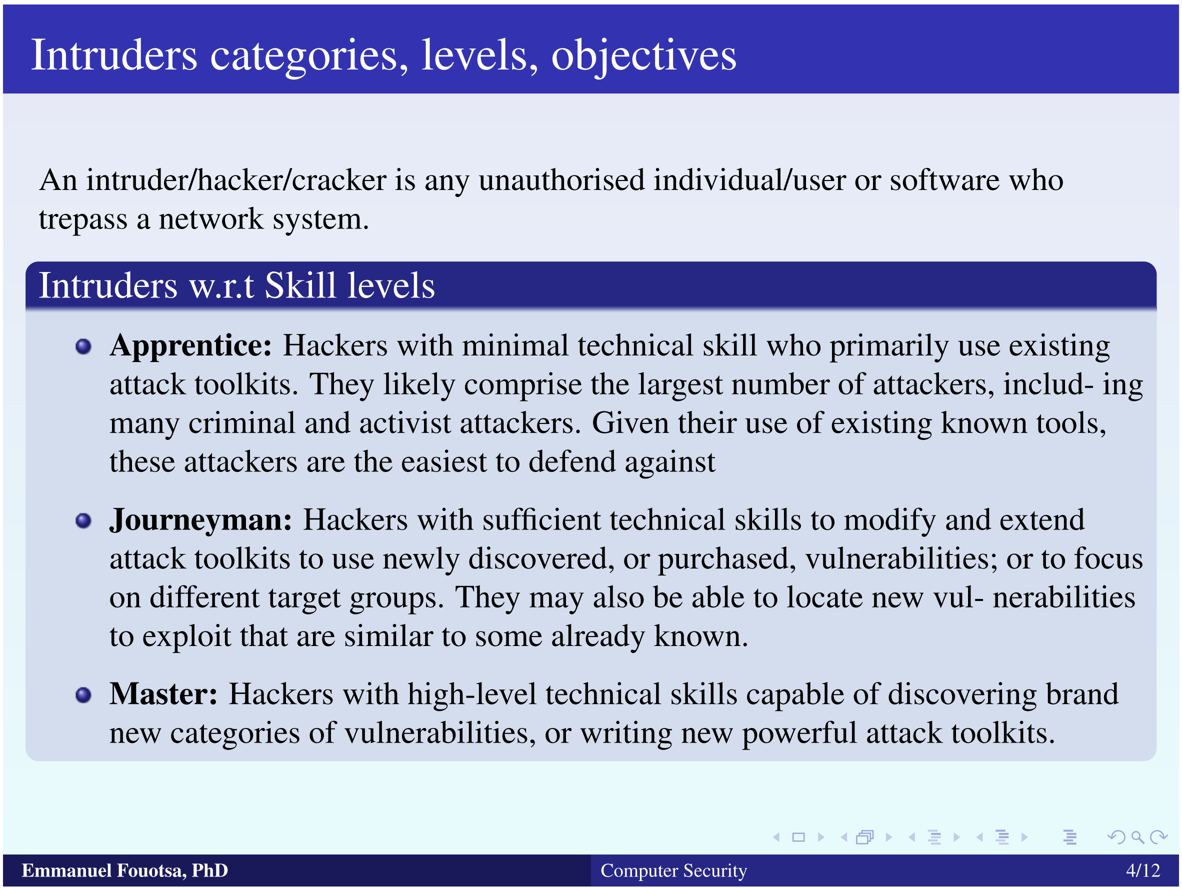


Intruders categories, levels, objectives

An intruder/hacker/cracker is any unauthorised individual/user or software who trepass a network system.

Classification of intruders

- **Cyber criminals:** Are either individuals or members of an organized crime group with a goal of financial reward. To achieve this, their activities may include identity theft, theft of financial credentials, corporate espionage, data theft, or data ransomin.
- **State-sponsored organizations** : Are groups of hackers sponsored by governments to conduct espionage or sabotage activities.
- **Activists:** Are either individuals, usually working as insiders, or members of a larger group of outsider attackers, who are motivated by social or political causes. They are also known as hacktivists, and their skill level is often quite low. The aim of their attacks is often to promote and publicize their cause, typically through website defacement, denial of service attacks, or the theft and distribution of data that results in negative publicity or compromise of their targets.

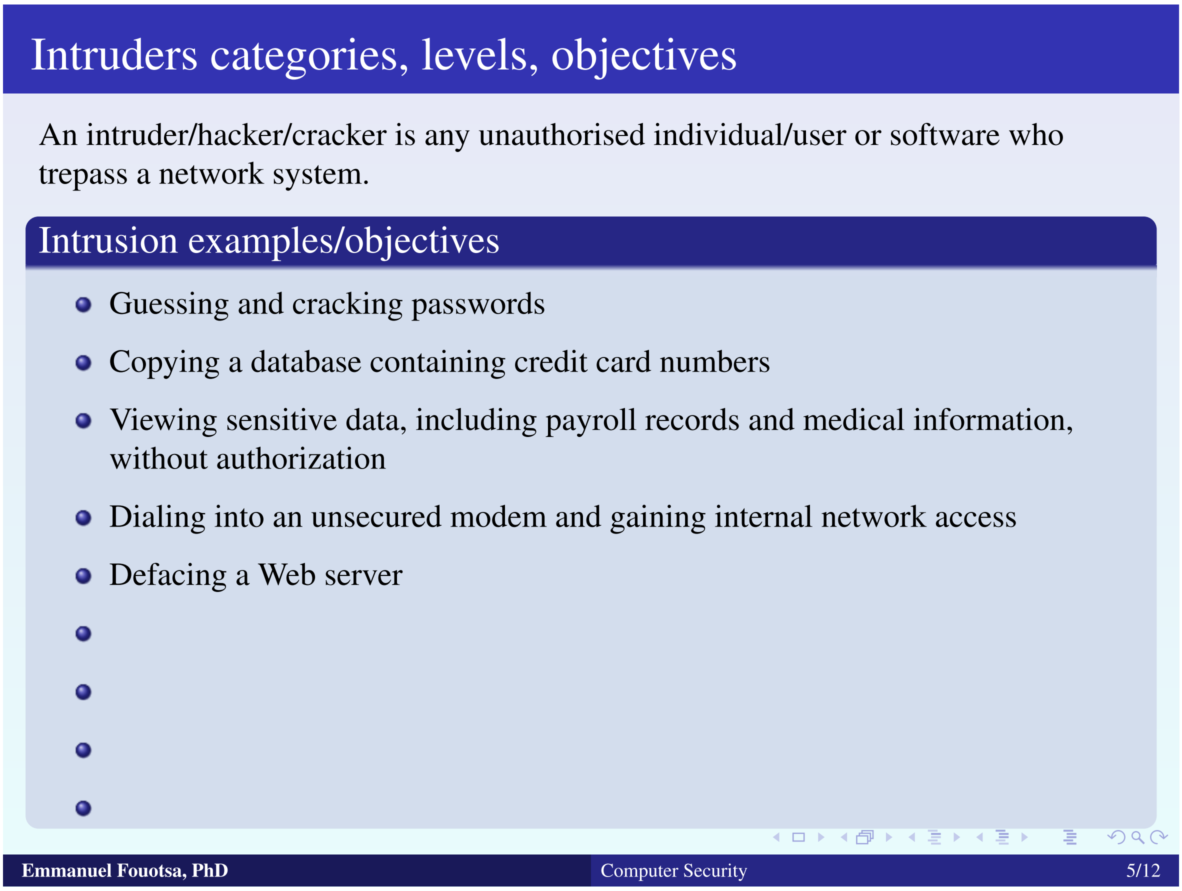


Intruders categories, levels, objectives

An intruder/hacker/cracker is any unauthorised individual/user or software who trepass a network system.

Intruders w.r.t Skill levels

- **Apprentice:** Hackers with minimal technical skill who primarily use existing attack toolkits. They likely comprise the largest number of attackers, includ- ing many criminal and activist attackers. Given their use of existing known tools, these attackers are the easiest to defend against
- **Journeyman:** Hackers with sufficient technical skills to modify and extend attack toolkits to use newly discovered, or purchased, vulnerabilities; or to focus on different target groups. They may also be able to locate new vul- nerabilities to exploit that are similar to some already known.
- **Master:** Hackers with high-level technical skills capable of discovering brand new categories of vulnerabilities, or writing new powerful attack toolkits.

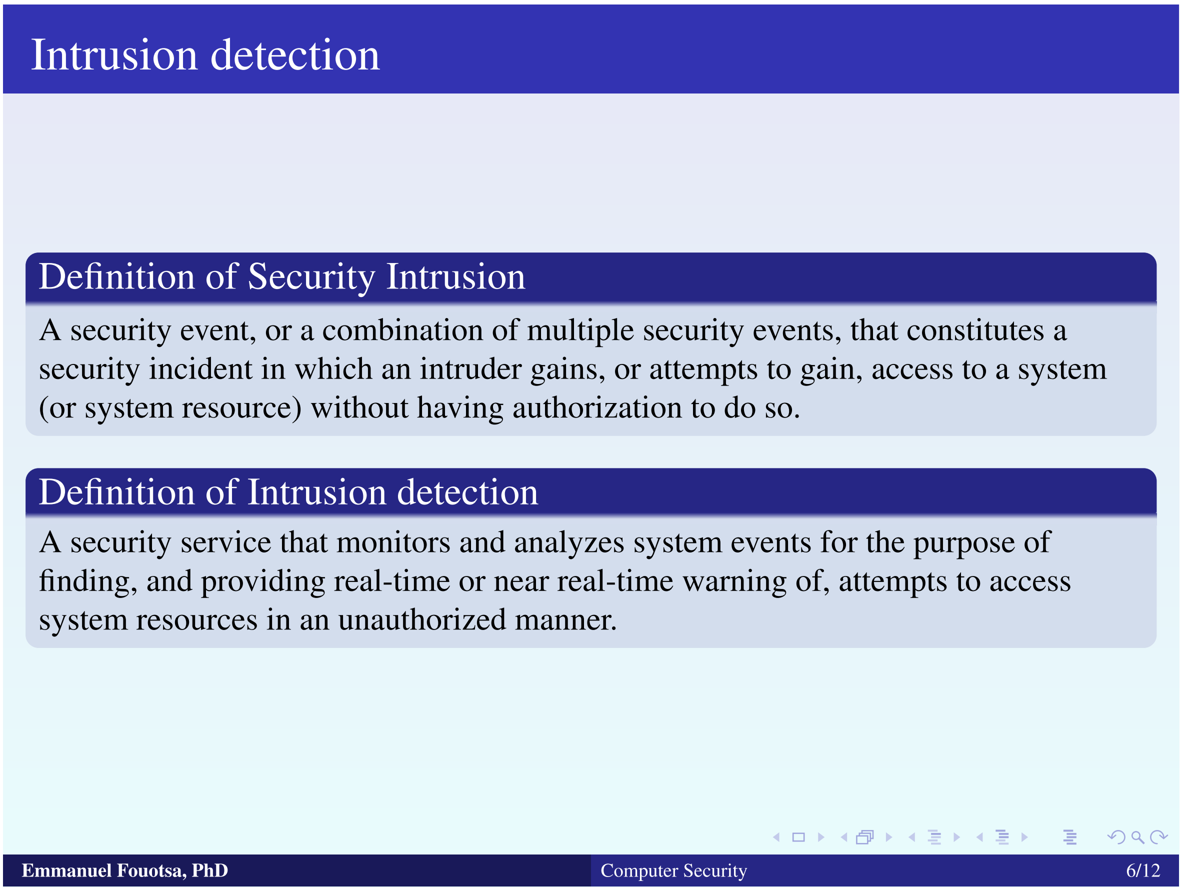


Intruders categories, levels, objectives

An intruder/hacker/cracker is any unauthorised individual/user or software who trepass a network system.

Intrusion examples/objectives

- Guessing and cracking passwords
- Copying a database containing credit card numbers
- Viewing sensitive data, including payroll records and medical information, without authorization
- Dialing into an unsecured modem and gaining internal network access
- Defacing a Web server
-
-
-
-



Intrusion detection

Definition of Security Intrusion

A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so.

Definition of Intrusion detection

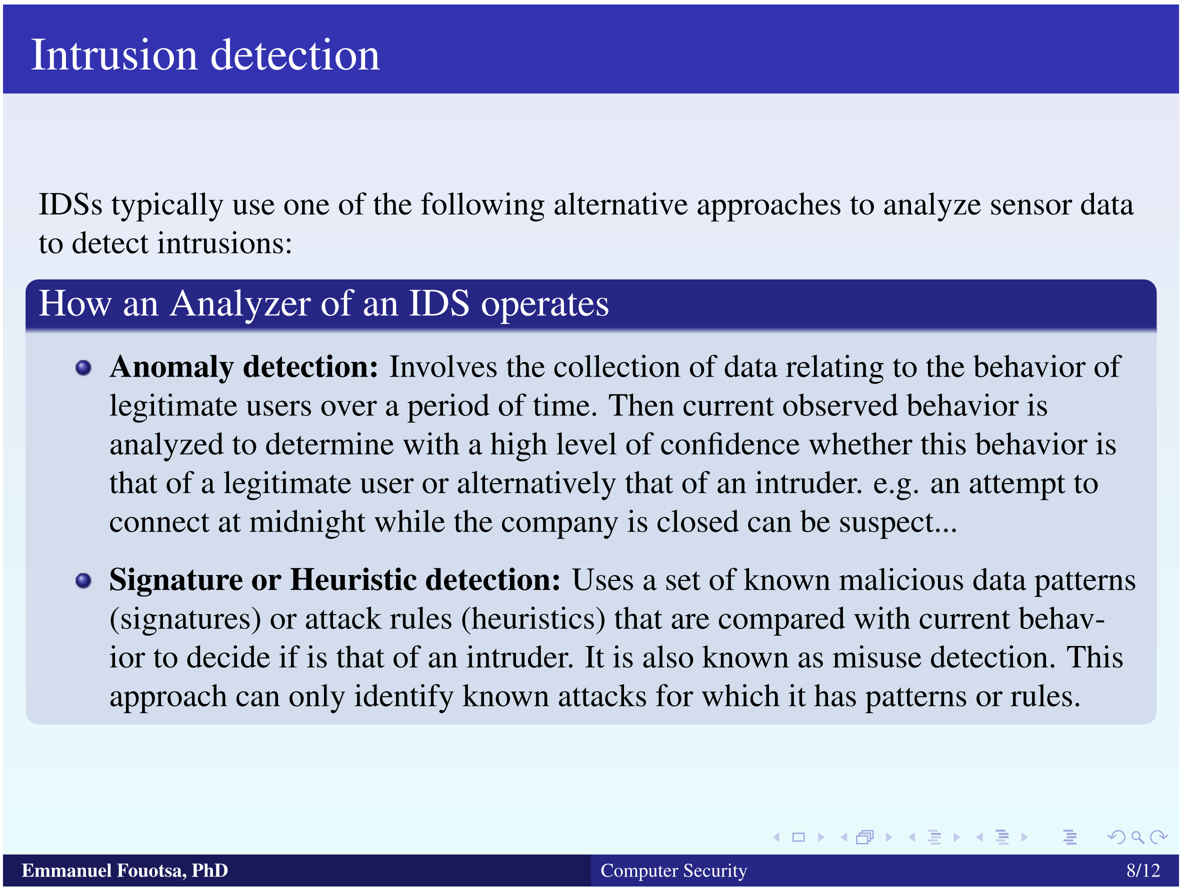
A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.

Intrusion detection

An IDS comprises three logical components:

Components of an Intrusion detection System (IDS)

- **Sensors:** Sensors are responsible for collecting data. The input for a sensor may be any part of a system that could contain evidence of an intrusion. Types of input to a sensor includes network packets, log files, and system call traces. Sensors collect and forward this information to the analyzer.
- **Analysers:** Analyzers receive input from one or more sensors or from other analyzers. The analyzer is responsible for determining if an intrusion has occurred. The output of this component is an indication that an intrusion has occurred. The output may include evidence supporting the conclusion that an intrusion occurred. The analyzer may provide guidance about what actions to take as a result of the intrusion. (see next page how analyzers operate)
- **user Interface:** The user interface to an IDS enables a user to view output from the system or control the behavior of the system.



Intrusion detection

IDSs typically use one of the following alternative approaches to analyze sensor data to detect intrusions:

How an Analyzer of an IDS operates

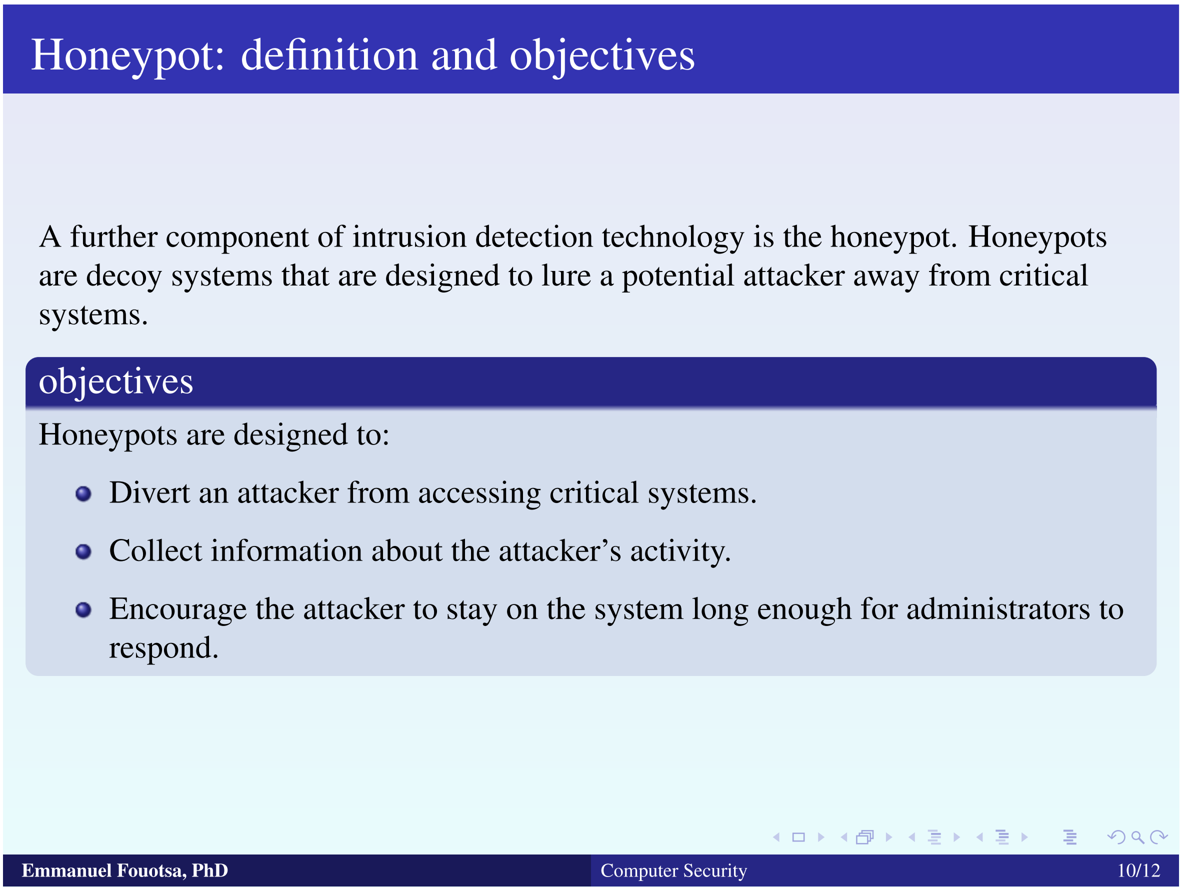
- **Anomaly detection:** Involves the collection of data relating to the behavior of legitimate users over a period of time. Then current observed behavior is analyzed to determine with a high level of confidence whether this behavior is that of a legitimate user or alternatively that of an intruder. e.g. an attempt to connect at midnight while the company is closed can be suspect...
- **Signature or Heuristic detection:** Uses a set of known malicious data patterns (signatures) or attack rules (heuristics) that are compared with current behavior to decide if is that of an intruder. It is also known as misuse detection. This approach can only identify known attacks for which it has patterns or rules.

Intrusion detection

IDSs are often classified based on the source and type of data analyzed, as:

Classification of Intrusion detection System (IDS)

- **Host-based IDS (HIDS):** Monitors the characteristics of a single host and the events occurring within that host, such as process identifiers and the system calls they make, for evidence of suspicious activity.
- **Network-based IDS (NIDS):** Monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity.
- **Distributed or hybrid IDS:** ombines information from a number of sensors, often both host and network-based, in a central analyzer that is able to better identify and respond to intrusion activity.



Honeypot: definition and objectives

A further component of intrusion detection technology is the honeypot. Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems.

objectives

Honeypots are designed to:

- Divert an attacker from accessing critical systems.
- Collect information about the attacker's activity.
- Encourage the attacker to stay on the system long enough for administrators to respond.

Honeypot: definition and objectives

Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems.

Principle of Honeypots

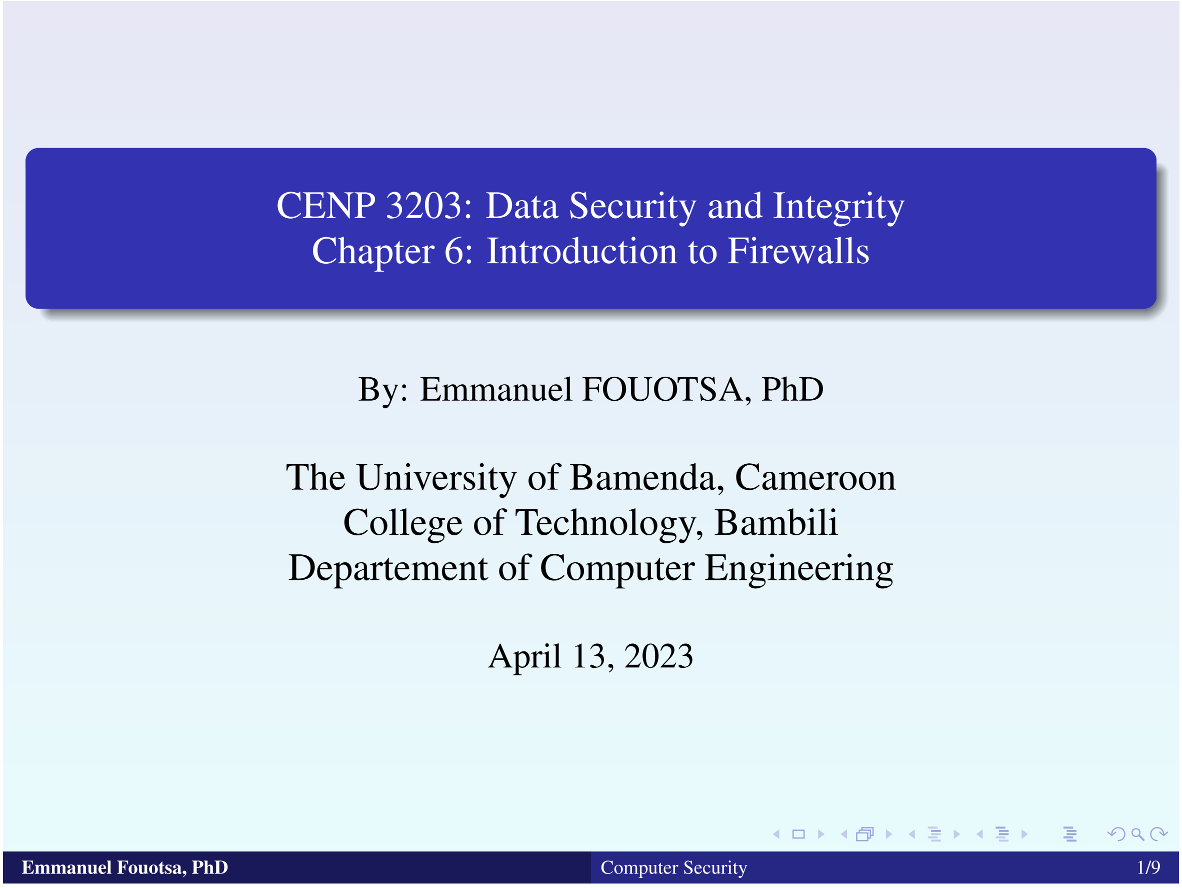
- are filled with fabricated information designed to appear valu- able but that a legitimate user of the system would not access. Thus, any access to the honeypot is suspect. The system is instrumented with sensitive monitors and event loggers that detect these accesses and collect information about the attacker's activities. Because any attack against the honeypot is made to seem successful, administrators have time to mobilize and log and track the attacker without ever exposing productive systems.
- The honeypot is a resource that has no production value. There is no legiti- mate reason for anyone outside the network to interact with a honeypot. Thus, any attempt to communicate with the system is most likely a probe, scan, or attack

The practice of the IDS Snort

Snort is an open source, highly configurable and portable host-based or network-based IDS.

Snort: an IDS

The practice of the Intrusion Detection System Snort: www.snort.org

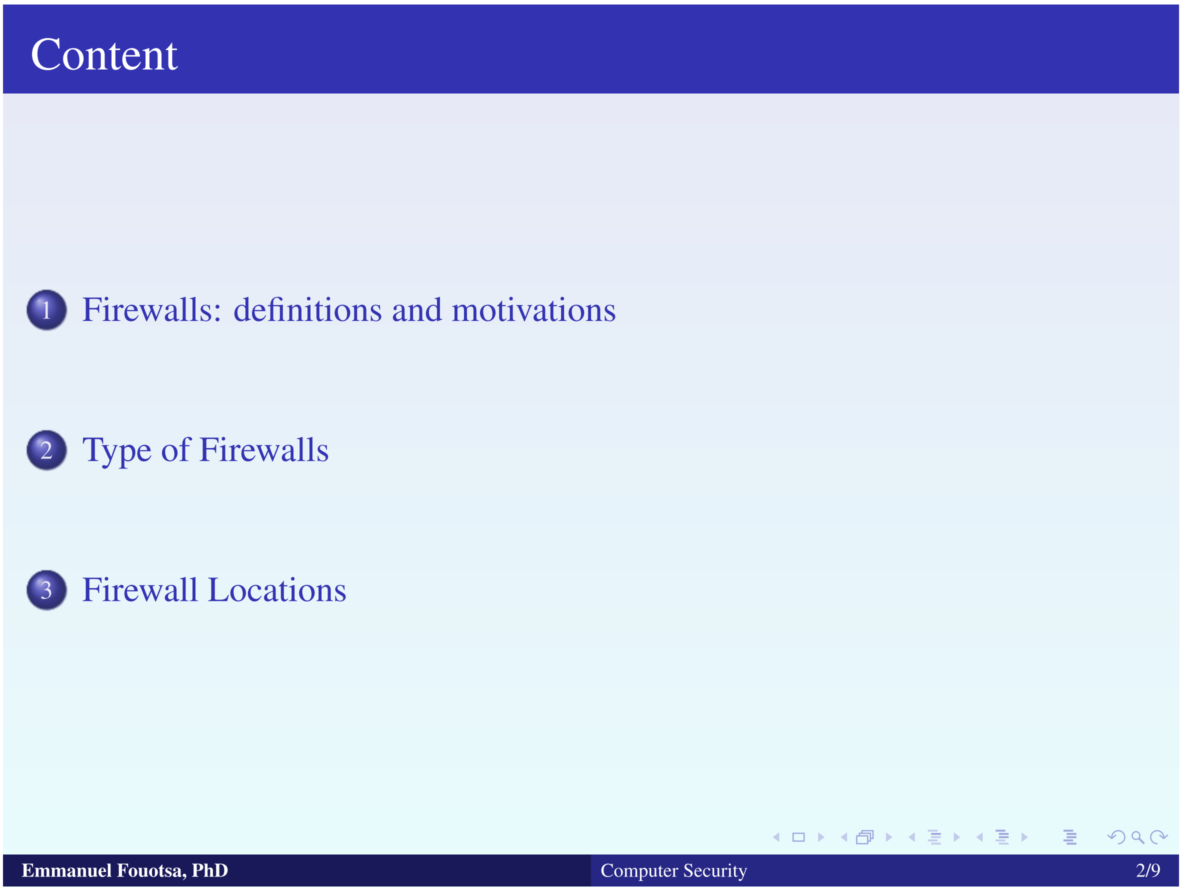


CENP 3203: Data Security and Integrity
Chapter 6: Introduction to Firewalls

By: Emmanuel FOUOTSA, PhD

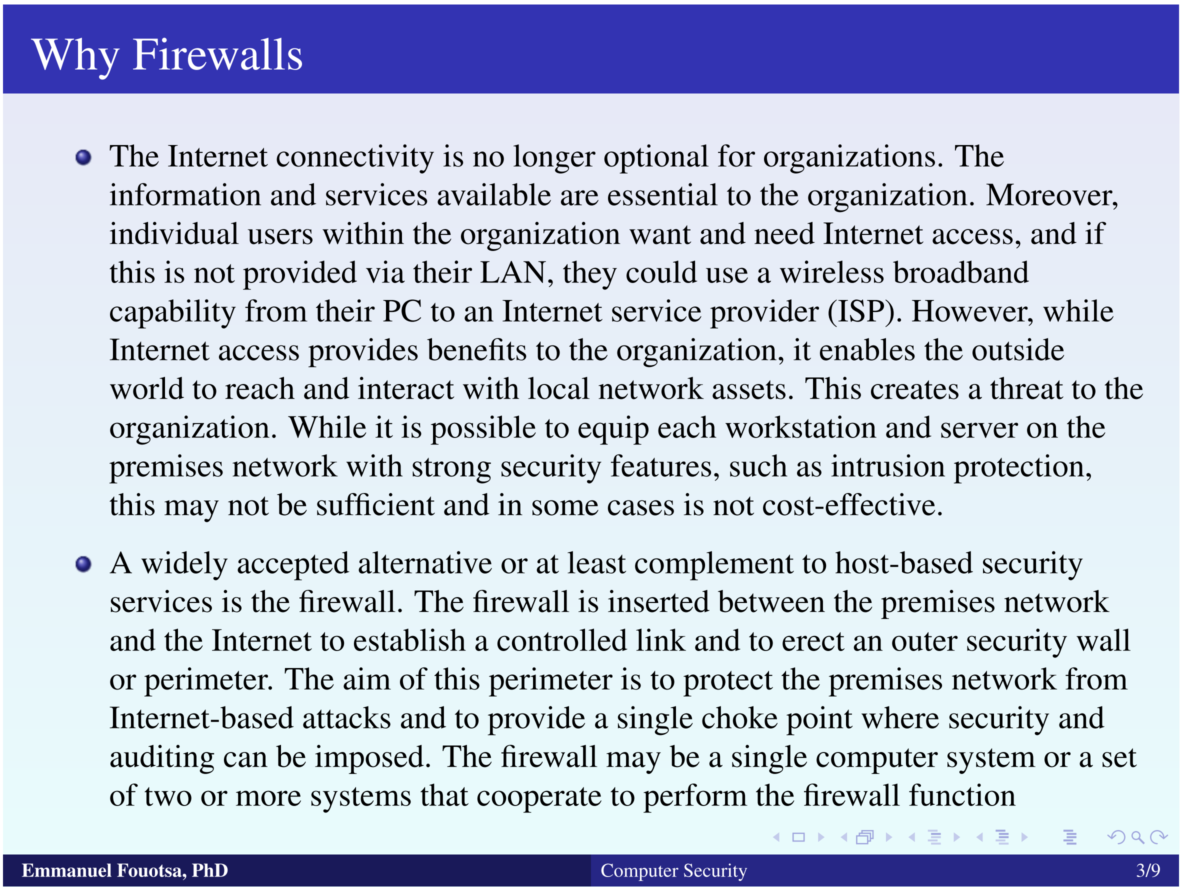
The University of Bamenda, Cameroon
College of Technology, Bambili
Departement of Computer Engineering

April 13, 2023



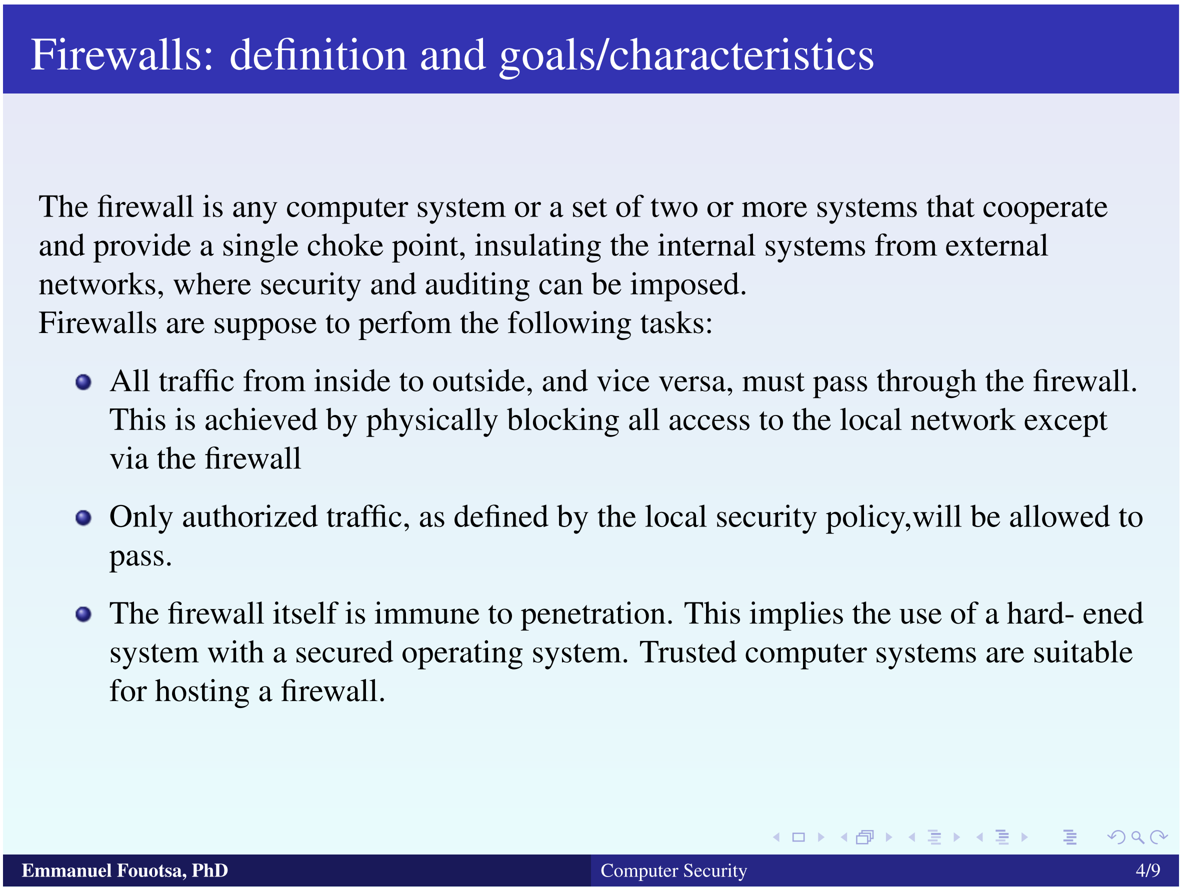
Content

1. Firewalls: definitions and motivations
2. Type of Firewalls
3. Firewall Locations



Why Firewalls

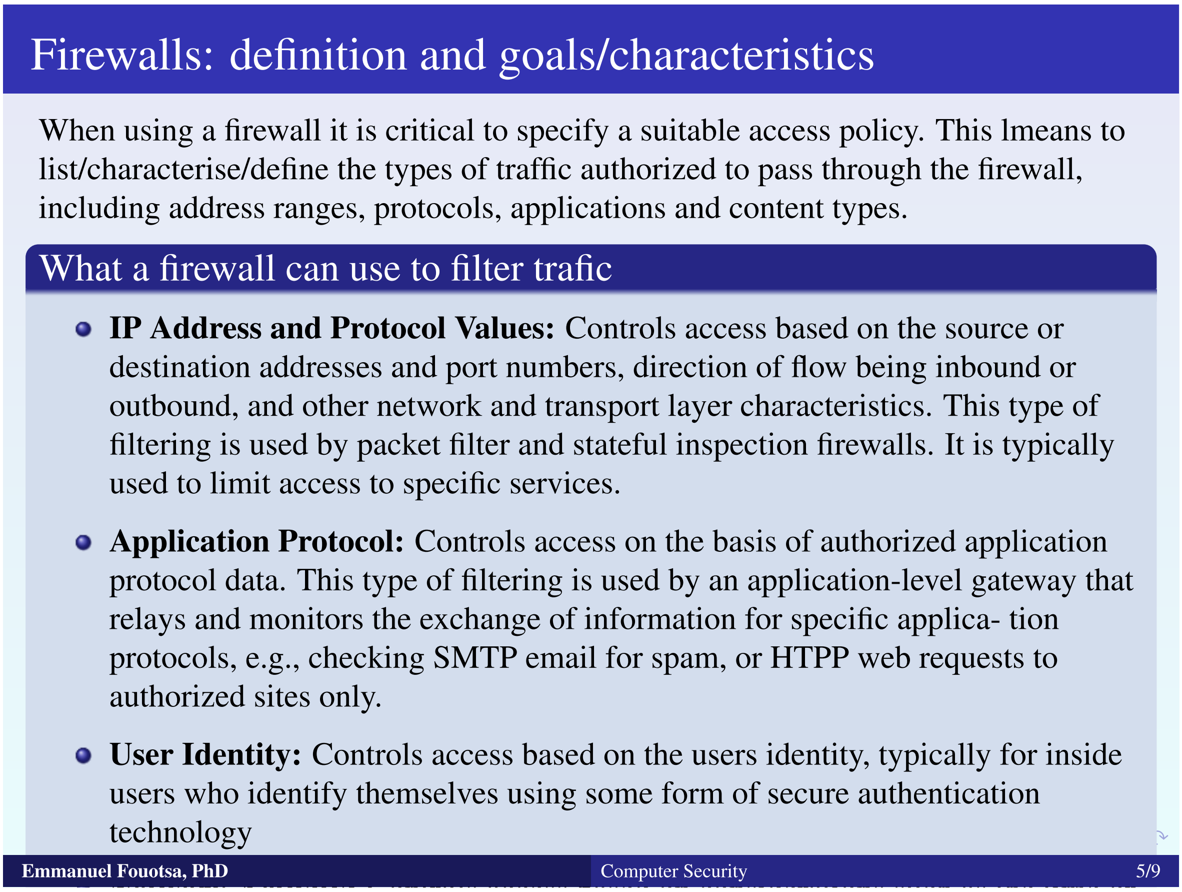
- The Internet connectivity is no longer optional for organizations. The information and services available are essential to the organization. Moreover, individual users within the organization want and need Internet access, and if this is not provided via their LAN, they could use a wireless broadband capability from their PC to an Internet service provider (ISP). However, while Internet access provides benefits to the organization, it enables the outside world to reach and interact with local network assets. This creates a threat to the organization. While it is possible to equip each workstation and server on the premises network with strong security features, such as intrusion protection, this may not be sufficient and in some cases is not cost-effective.
- A widely accepted alternative or at least complement to host-based security services is the firewall. The firewall is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter. The aim of this perimeter is to protect the premises network from Internet-based attacks and to provide a single choke point where security and auditing can be imposed. The firewall may be a single computer system or a set of two or more systems that cooperate to perform the firewall function



Firewalls: definition and goals/characteristics

The firewall is any computer system or a set of two or more systems that cooperate and provide a single choke point, insulating the internal systems from external networks, where security and auditing can be imposed.
Firewalls are suppose to perfom the following tasks:

- All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall
- Only authorized traffic, as defined by the local security policy,will be allowed to pass.
- The firewall itself is immune to penetration. This implies the use of a hard- ened system with a secured operating system. Trusted computer systems are suitable for hosting a firewall.



Firewalls: definition and goals/characteristics

When using a firewall it is critical to specify a suitable access policy. This lmeans to list/characterise/define the types of traffic authorized to pass through the firewall, including address ranges, protocols, applications and content types.

What a firewall can use to filter trafic

- **IP Address and Protocol Values:** Controls access based on the source or destination addresses and port numbers, direction of flow being inbound or outbound, and other network and transport layer characteristics. This type of filtering is used by packet filter and stateful inspection firewalls. It is typically used to limit access to specific services.
- **Application Protocol:** Controls access on the basis of authorized application protocol data. This type of filtering is used by an application-level gateway that relays and monitors the exchange of information for specific applica- tion protocols, e.g., checking SMTP email for spam, or HTPP web requests to authorized sites only.
- **User Identity:** Controls access based on the users identity, typically for inside users who identify themselves using some form of secure authentication technology

Type of Firewalls

A firewall can monitor network traffic at a number of levels, from low-level network packets, either individually or as part of a flow, to all traffic within a transport connection, up to inspecting details of application protocols. The choice of which level is appropriate is determined by the desired firewall access policy.

1-A packet filtering firewall

A packet filtering firewall: applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet. The firewall is typically configured to filter packets going in both directions (from and to the internal network). Filtering rules are based on information contained in a network packet:

- **Source IP address:** The IP address of the system that originated the IP packet (e.g., 192.178.1.1).
- **Destination IP address:** The IP address of the system the IP packet is trying to reach (e.g., 192.168.1.2).
- **Source and destination transport-level address:** The transport-level (e.g., TCP or UDP) port number, which defines applications such as SNMP or TELNET.
- **IP protocol field:** Defines the transport protocol
- **Interface:** For a firewall with three or more ports, which interface of the firewall the packet came from or which interface of the firewall the packet is destined for.

Type of Firewalls

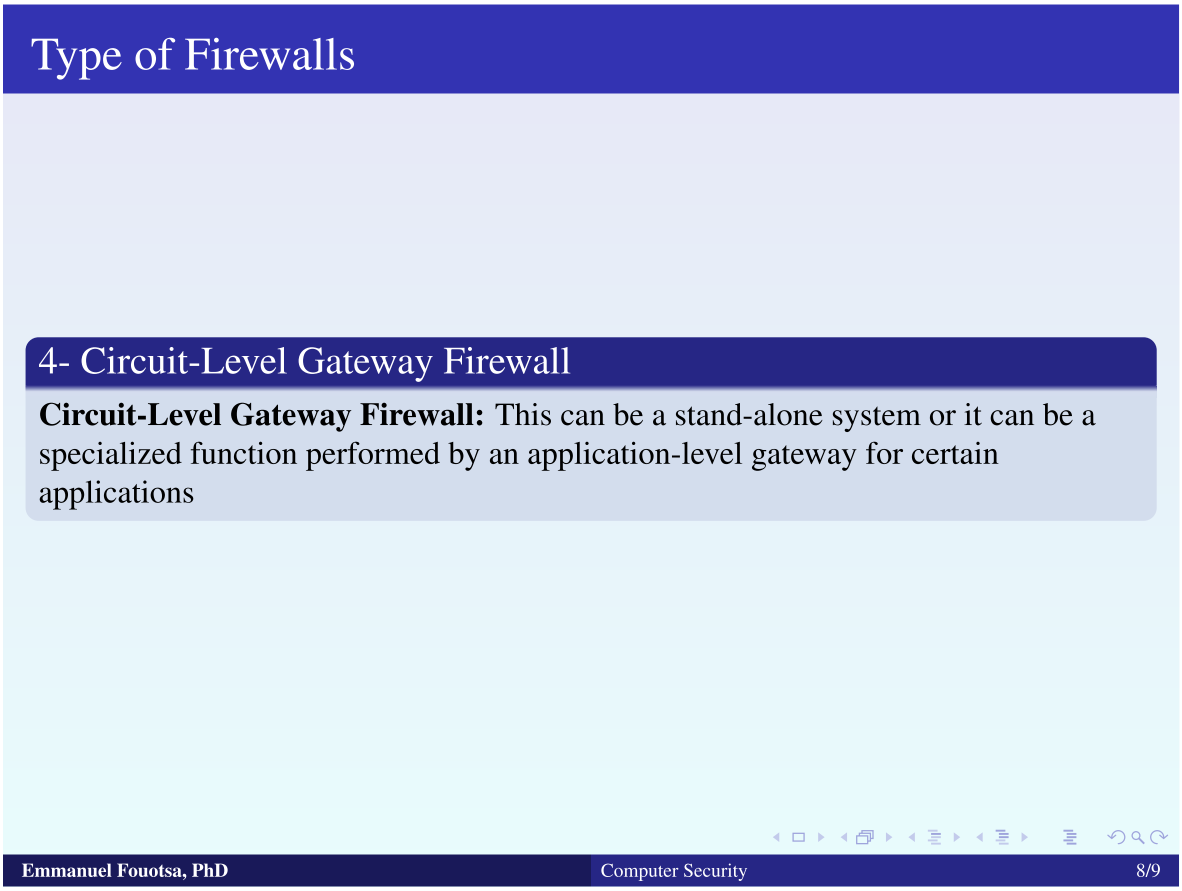
Exercise: Enumerate some of the attacks that can be made on packet filtering firewalls and the appropriate countermeasures.

2-Stateful Inspection Firewalls

Stateful Inspection Firewalls: A stateful packet inspection firewall reviews the same packet information as a packet filtering firewall, but also records information about TCP connections.

3-Application-Level Gateway

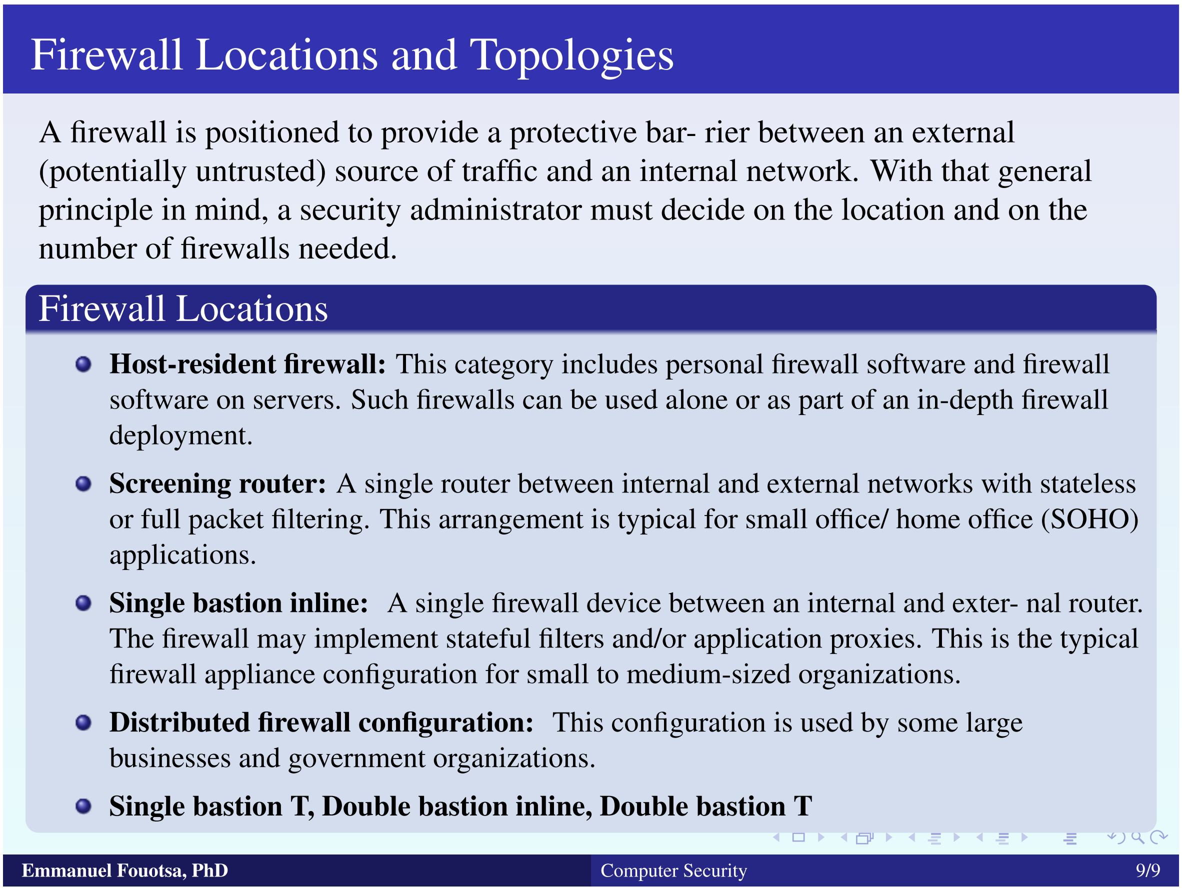
Application-Level Gateway: also called an application proxy, acts as a relay of application-level traffic . The user contacts the gateway using a TCP/ IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints. If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall



Type of Firewalls

4- Circuit-Level Gateway Firewall

Circuit-Level Gateway Firewall: This can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications



Firewall Locations and Topologies

A firewall is positioned to provide a protective bar- rier between an external (potentially untrusted) source of traffic and an internal network. With that general principle in mind, a security administrator must decide on the location and on the number of firewalls needed.

Firewall Locations

- **Host-resident firewall:** This category includes personal firewall software and firewall software on servers. Such firewalls can be used alone or as part of an in-depth firewall deployment.
- **Screening router:** A single router between internal and external networks with stateless or full packet filtering. This arrangement is typical for small office/ home office (SOHO) applications.
- **Single bastion inline:** A single firewall device between an internal and exter- nal router. The firewall may implement stateful filters and/or application proxies. This is the typical firewall appliance configuration for small to medium-sized organizations.
- **Distributed firewall configuration:** This configuration is used by some large businesses and government organizations.
- **Single bastion T, Double bastion inline, Double bastion T**